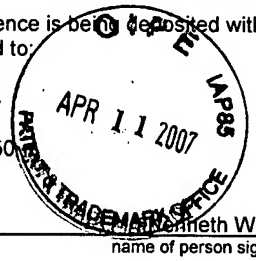
CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450



Kenneth W. Fields
name of person signing certification

Signature

April 9, 2007
Date

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	**Confirmation No. 4067**
Kaoru MURASE et al.	:	Attorney Docket No. 2002_0184A
Serial No. 10/066,725	:	Group Art Unit 2131
Filed February 6, 2002	:	Examiner Matthew T. Henning
DATA NULLIFICATION DEVICE FOR NULLIFYING DIGITAL CONTENT RECORDED ON A RECORDING MEDIUM, AFTER THE DIGITAL CONTENT HAS BEEN REPRODUCED, A PREDETERMINED TIME PERIOD HAS PASSED SINCE THE RECORDING OF THE DIGITAL CONTENT, OR THE DIGITAL CONTENT HAS BEEN MOVED TO ANOTHER RECORDING MEDIUM	:	**Mail Stop: Amendment**

THE COMMISIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 29-0875

SUBMISSION OF VERIFIED ENGLISH TRANSLATION OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Attached hereto is a verified English translation of the foreign priority document (JP Application No. 2001-039140) for the present application.

If the Examiner has any questions regarding this document, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Kaoru MURASE et al.

By: Kenneth W. Fields

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/jjv
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 9, 2007

VERIFICATION OF TRANSLATION

I, Sachiko Takagi, translator of Suita, Osaka, Japan, hereby declare that I am conversant with the English and Japanese languages and am a competent translator thereof. I further declare that to the best of my knowledge and belief the following is a true and correct translation made by me of Japanese Patent Application No. 2001-039140 filed on February 15, 2001.

Date: March 27, 2007

Sachiko Takagi

SACHIKO TAKAGI

[Title of the Document] Patent Application

[Our Reference Number] 2022520583

[Application Date] February 15, 2001

[Direction] Commissioner, Patent Office

[Classification of International Patent] G09C 1/00

[Inventor]

[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006, OazaKadoma, Kadoma-shi, Osaka

[Name] Kaoru Murase

[Inventor]

[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006, OazaKadoma, Kadoma-shi, Osaka

[Name] Yoshihiko Motohashi

[Inventor]

[Address or Residence] c/o MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd. 1006, OazaKadoma, Kadoma-shi, Osaka

[Name] Masaya Miyazaki

[Applicant]

[Identification Number] 000005821

[Name] MATSUSHITA ELECTRIC INDUSTRIAL Co., Ltd

[Patent Attorney]

[Identification Number] 100090446

[Name] Shiro Nakajima

[Payment]

[Prepayment Registration Number] 014823

[Filing Fee] ¥21000

[List of Enclosures]

[Document] Specification 1

[Document] Drawing 1

[Document] Abstract 1

[Power of Attorney/Reference No.] 9003742

Document Specification

Name of the Invention

DATA NULLIFICATION DEVICE

Range of the Patent Claims

Claim 1

A data nullification device for nullifying target data recorded on a recording medium,

the target data being made up of a plurality of data blocks,

the data nullification device being characterized by comprising:

a judging unit operable to judge, for each data block recorded on the recording medium, whether the data block needs to be nullified; and

a nullifying unit operable to sequentially nullify, when a predetermined number of data blocks or a predetermined amount of data of data blocks are judged as needing to be nullified, the judged data blocks of the target data recorded on the recording medium.

Claim 2

The data nullification device of Claim 1,

wherein the recording medium stores sequence

information that shows a sequence in which the plurality of data blocks are recorded onto the recording medium, and

the judging unit judges, in succession, the plurality of data blocks in the sequence shown by the sequence information, as needing to be nullified.

Claim 3

The data nullification device of Claim 2,

wherein the target data recorded on the recording medium is data which is continuously transmitted from an external device and recorded on the recording medium,

the data nullification device further comprises:

a receiving unit operable to receive data from the external device, and

having set the received data as a new data block, the nullifying unit writes the new data block to a recording area, on the recording medium, that stores a data block which is judged as needing to be nullified, to nullify the recorded data block and at the same time record the new data block.

Claim 4

The data nullification device of Claim 3,

wherein each data block has a length corresponding to a fixed transmission time period, and

a specified number of recording areas which are each used as a recording area of a data block are reserved on the recording medium.

Claim 5

The data nullification device of Claim 4,

wherein if the length corresponding to the fixed transmission time period is variable and if part of the recorded data block remains even after the new data block is written, the nullifying unit further writes arbitrary data over the part of the recorded data block.

Claim 6

The data nullification device of one of Claims 4 and 5,

wherein if there is not a new data block which is to be recorded, the nullifying unit writes arbitrary data to the recording area.

Claim 7

The data nullification device of Claim 1,

wherein the recording medium stores time limit information showing a recording time limit of each data block recorded on the recording medium, the recording time limit

being a time limit after which retention of the data block on the recording medium is prohibited, and

the judging unit judges that each data block whose recording time limit is reached needs to be nullified, based on the time limit information.

Claim 8

The data nullification device of one of Claims 2 and 7, further comprising:

a utilizing unit operable to utilize the target data recorded on the recording medium, in units of data blocks,

wherein the judging unit further judges that each data block which was utilized by the utilizing unit needs to be nullified.

Claim 9

The data nullification device of Claim 1, further comprising:

a utilizing unit operable to utilize the target data recorded on the recording medium, in units of data blocks,

wherein the judging unit further judges that each data block which was utilized by the utilizing unit needs to be nullified.

Claim 10

The data nullification device of one of Claims 8 and 9,

wherein the target data recorded on the recording medium is content data which is transmitted from an external device and recorded on the recording medium,

the content data is accompanied with copy control information showing whether copying of the content data is permitted or prohibited,

the utilizing unit reproduces the content data recorded on the recording medium, in units of data blocks, and

only if the copy control information accompanying the content data shows that the copying of the content data is prohibited, the judging unit judges that each data block which was reproduced by the utilizing unit needs to be nullified.

Claim 11

The data nullification device of Claim 9,

wherein the target data recorded on the recording medium is accompanied with copy control information showing whether copying of the target data is permitted or prohibited,

the utilizing unit records the target data recorded on the recording medium, to another recording medium, in units of data blocks, and

only if the copy control information accompanying the target data shows that the copying of the target data is prohibited, the judging unit judges that each data block on the recording medium which corresponds to a data block recorded to the other recording medium by the utilizing unit needs to be nullified.

Claim 12

The data nullification device of one of Claims 1 to 11,

wherein the nullifying unit destroys all parts of a data block which is judged as needing to be nullified.

Claim 13

The data nullification device of one of Claims 1, 2, and 7 to 11,

wherein the nullifying unit destroys at least a part of a data block which is judged as needing to be nullified, the part of the data block being necessary to utilize remaining parts of the data block.

Claim 14

The data nullification device of Claim 13,

wherein the target data recorded on the recording medium is MPEG data including I pictures, and

the part of the data block necessary to utilize the remaining parts of the data block is an I picture.

Claim 15

The data nullification device of Claim 13,

wherein the target data recorded on the recording medium is MPEG data including I pictures, and

the part of the data block necessary to utilize the remaining parts of the data block is a first sector of an I picture.

Claim 16

The data nullification device of one of Claims 13 to 15,

wherein when the data nullification device does not have an enough processing capacity, the nullifying unit destroys only the part of the data block necessary to utilize the remaining parts of the data block.

Claim 17

The data nullification device of Claim 16,

wherein the nullifying unit destroys the remaining parts of the data block within a range where a processing capacity of the data nullification device allows.

Claim 18

The data nullification device of one of Claims 16 and 17, further comprising:

a total destroying unit operable to destroy remaining parts of data blocks which were not destroyed by the nullifying unit, when the data nullification device has an enough processing capacity.

Claim 19

The data nullification device of one of Claims 1, 2, and 7 to 11,

wherein each data block recorded on the recording medium has been encrypted using an individual data block encryption key,

a data block decryption key for decrypting the encrypted data block is stored on the recording medium, and

the nullifying unit destroys at least a data block decryption key, on the recording medium, corresponding to a data block which is judged as needing to be nullified.

Claim 20

The data nullification device of Claim 19, further

comprising:

an acquiring unit operable to acquire the target data in an encrypted form;

a decrypting unit operable to decrypt the encrypted target data using a user key which has been provided to authorized users in advance, to obtain the target data;

a key generating unit operable to generate an arbitrary data block encryption key and a data block decryption key corresponding to the data block encryption key, for each data block of the target data;

a data encrypting unit operable to encrypt the data block using the data block encryption key so that the encrypted data block can be decrypted using the corresponding data block decryption key;

a key encrypting unit operable to encrypt the data block decryption key using an identifier unique to the data nullification device; and

a recording unit operable to record the encrypted data block and the encrypted data block decryption key onto the recording medium.

Claim 21

The data nullification device of Claim 20,

wherein at least the decrypting unit, the key generating unit, the data encrypting unit, and the key

encrypting unit are contained in a single semiconductor chip.

Claim 22

A data nullification program for nullifying target data recorded on a recording medium,

the target data being made up of a plurality of data blocks,

the data nullification program being characterized by having a computer execute:

a judging step of judging, for each data block recorded on the recording medium, whether the data block needs to be nullified; and

a nullifying step of sequentially nullifying, when a predetermined number of data blocks or a predetermined amount of data of data blocks are judged as needing to be nullified, the judged data blocks.

Claim 23

The data nullification program of Claim 22,

wherein the recording medium stores sequence information that shows a sequence in which the plurality of data blocks are recorded onto the recording medium, and

the judging step judges, in succession, the plurality

of data blocks in the sequence shown by the sequence information, as needing to be nullified.

Claim 24

The data nullification program of Claim 23,

wherein the target data recorded on the recording medium is data which is continuously transmitted from an external device and recorded on the recording medium,

the data nullification program further having the computer execute:

a receiving step of receiving data from the external device,

wherein having set the received data as a new data block, the nullifying step writes the new data block to a recording area, on the recording medium, that stores a data block which is judged as needing to be nullified, to nullify the recorded data block and at the same time record the new data block.

Claim 25

The data nullification program of Claim 22,

wherein the recording medium stores time limit information showing a recording time limit of each data block recorded on the recording medium, the recording time limit being a time limit after which retention of the data

block on the recording medium is prohibited,

the judging step judges that each data block whose recording time limit is reached needs to be nullified, based on the time limit information.

Claim 26

The data nullification program of one of Claims 23 and 25, further having the computer execute:

a utilizing step of utilizing the target data recorded on the recording medium, in units of data blocks,

wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

Claim 27

The data nullification program of Claim 22, further having the computer execute:

a utilizing step of utilizing the target data recorded on the recording medium, in units of data blocks,

wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

Claim 28

The data nullification program of one of Claims 22

to 27,

wherein the nullifying step destroys all parts of a data block which is judged as needing to be nullified.

Claim 29

The data nullification program of one of Claims 22, 23, and 25 to 27,

wherein the nullifying step destroys at least a part of a data block which is judged as needing to be nullified, the part of the data block being necessary to utilize remaining parts of the data block.

Claim 30

The data nullification program of one of Claims 22, 23, and 25 to 27,

wherein each data block recorded on the recording medium has been encrypted using an individual data block encryption key,

a data block decryption key for decrypting the encrypted data block is stored on the recording medium, and

the nullifying step destroys at least a data block decryption key, on the recording medium, corresponding to a data block which is judged as needing to be nullified.

Claim 31

A data nullification method for nullifying target data recorded on a recording medium,

the target data being made up of a plurality of data blocks,

the data nullification method being characterized by comprising:

a judging step of judging, for each data block recorded on the recording medium, whether the data block needs to be nullified; and

a nullifying step of sequentially nullifying, when a predetermined number of data blocks or a predetermined amount of data of data blocks are judged as needing to be nullified, the judged data blocks.

Claim 32

The data nullification method of Claim 31,

wherein the recording medium stores sequence information that shows a sequence in which the plurality of data blocks are recorded onto the recording medium, and

the judging step judges, in succession, the plurality of data blocks in the sequence shown by the sequence information, as needing to be nullified.

Claim 33

The data nullification method of Claim 32,

wherein the target data recorded on the recording medium is data which is continuously transmitted from an external device and recorded on the recording medium,

the data nullification method further comprising:

a receiving step of receiving data from the external device,

wherein having set the received data as a new data block, the nullifying step writes the new data block to a recording area, on the recording medium, that stores a data block which is judged as needing to be nullified, to nullify the recorded data block and at the same time record the new data block.

Claim 34

The data nullification method of Claim 31,

wherein the recording medium stores time limit information showing a recording time limit of each data block recorded on the recording medium, the recording time limit being a time limit after which retention of the data block on the recording medium is prohibited, and

the judging step judges that each data block whose recording time limit is reached needs to be nullified, based on the time limit information.

Claim 35

The data nullification method of one of Claims 32 and 34, further comprising:

a utilizing step of utilizing the target data recorded on the recording medium, in units of data blocks,

wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

Claim 36

The data nullification method of Claim 31, further comprising:

a utilizing step of utilizing the target data recorded on the recording medium, in units of data blocks,

wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

Claim 37

The data nullification method of one of Claims 31 to 36,

wherein the nullifying step destroys all parts of a data block which is judged as needing to be nullified.

Claim 38

The data nullification method of one of Claims 31, 32, and 34 to 36,

wherein the nullifying step destroys at least a part of a data block which is judged as needing to be nullified, the part of the data block being necessary to utilize remaining parts of the data block.

Claim 39

The data nullification method of one of Claims 31, 32, and 34 to 36,

wherein each data block recorded on the recording medium has been encrypted using an individual data block encryption key,

a data block decryption key for decrypting the encrypted data block is stored on the recording medium, and

the nullifying step destroys at least a data block decryption key, on the recording medium, corresponding to a data block which is judged as needing to be nullified.

DETAILED DESCRIPTION OF THE INVENTION

[0001]

Field of the Invention

The present invention relates to a device for

nullifying data to protect its copyright, and in particular relates to techniques for enhancing user convenience while protecting copyrighted data.

[0002]

Description of the Prior Art

The digitization of information is increasing in recent years. Since digitized information (hereafter referred to as "digital content") not only is relatively easy to handle but also does not degrade in quality with time, especially audio information and video information are becoming more and more digitized.

On the other hand, digital content can be copied to produce the exactly same one as the original. This provokes unauthorized acts such as illegal duplication or tampering of copyrighted information.

[0003]

To discourage such unauthorized acts, a method may be employed that encrypts digital content, and provides a decryption key for decrypting the encrypted digital content (hereafter simply referred to as "encrypted content") only to devices of authorized users who have agreed to pay copyright fees.

This prohibits the encrypted content from being decrypted using devices other than those of the authorized users. Hence the digital content can be protected from

unauthorized use.

[0004]

Also, there is a method for indicating the copyright protection status of digital content. According to this method, copy control information (CCI) that shows whether copying of the digital content is permitted or not is attached to the digital content.

In more detail, the copy control information shows one of four states that are "Copy Never", "Copy one Generation", "Copy No more", and "Copy Free".

[0005]

"Copy Never" means no copies of digital content are permitted.

"Copy one Generation" means only a first generation copy of digital content is permitted to be generated. The first generation copy of the digital content is given copy control information "Copy No more".

[0006]

"Copy No more" is copy control information that is attached to digital content which is a first generation copy of digital content whose copy control information is "Copy one Generation". "Copy No more" means copying is not permitted any more though it was permitted previously.

"Copy Free" means digital content can be copied

freely.

[0007]

In commercial digital broadcasting and the like, digital content is transmitted via a transmission line in the following manner. If the copy control information of the digital content is "Copy Never", "Copy one Generation", or "Copy No more", it is definitely transmitted in an encrypted form, to ensure security on the transmission line. If the copy control information of the digital content is "Copy Free", it is usually transmitted in an unencrypted form.

[0008]

Problem the Present Invention is Attempting to Solve

When the user obtains digital content whose copy control information is "Copy Never" via a transmission line and reproduces it, the user is prohibited from copying the obtained digital content to a recording medium. Also, when the user obtains digital content whose copy control information is "Copy one Generation" and records it onto a recording medium thereby generating digital content whose copy control information is "Copy No more", the user cannot copy the digital content recorded on the recording medium to another recording medium. In such cases where copying of digital content is completely prohibited, the user is likely to encounter a lot of inconveniences.

[0009]

If copying of digital content transmitted via a transmission line is permitted, the user can perform time-shifted viewing, i.e., the user can record the digital content to a recording medium on the receiver side for later viewing, or the user can record the digital content to a recording medium such as an HDD (hard disk drive) while reproducing it. However, in the case of digital content which cannot be copied, once the user stops viewing the digital content to go to the bathroom or to answer the telephone or bell, he or she cannot view the missed part unless the digital content is rebroadcast. Many movie films run for about two hours, and some feature length films even run for more than four hours. Also, commercial digital broadcasting and the like usually do not include commercials. Therefore, to view an entire movie film or the like which is marked as "Copy Never", i.e. which cannot be copied at all, the user cannot answer the phone or bell and cannot even go to the bathroom for the running time of the movie film that lasts two to four hours. This causes a great deal of inconvenience to the user.

[0010]

Also, if copying of digital content is still permitted after the user acquires the digital content and records it to a recording medium, the user can freely copy or move

the recorded digital content to another recording medium. However, in the case of digital content which cannot be copied, once the user has acquired the digital content and recorded it onto some recording medium, the user cannot move that digital content to another recording medium. Since it is convenient to use a fixed recording medium such as an HDD that is easy to use and quick to access, the user is likely to record the acquired digital content first of all to such a fixed recording medium. However, fixed recording media have only limited storage capacities. Also, general fixed recording media such as HDDs are more susceptible to breakage than removable recording media, as they tend to be constantly used. For these reasons, if the user views the digital content and wants to store it long-term, it is desirable to move the digital content to a removable recording medium, such as a DVD-RW or a digital videotape, that has a larger storage capacity and is more preferable for long-term storage.

[0011]

However, it is not acceptable, in terms of copyright protection, to alter the non-copyable status of the copyrighted digital content so as to improve user-friendliness.

In an ideal meaning, digital content whose copy control information is "Copy Never" can be viewed but cannot

be copied, and digital content whose copy control information is "Copy one Generation" can be copied only once.

[0012]

In view of this, it is desirable to allow copying of digital content under a specific condition but then reliably nullify the digital content. In this way, user-friendliness can be improved without departing from the principle of copy prohibition.

The present invention has an object of providing a data nullification device, a data nullification method, a data nullification program, and a computer-readable recording medium recording a data nullification program which enable user-friendliness to be improved without departing from the principle of copy prohibition.

[0013]

Means for Solving the Stated Problem

The stated object can be achieved by a data nullification device for nullifying target data recorded on a recording medium, the target data being made up of a plurality of data blocks, the data nullification device being characterized by including: a judging unit operable to judge, for each data block recorded on the recording medium, whether the data block needs to be nullified; and a nullifying unit operable to sequentially nullify, when

a predetermined number of data blocks or a predetermined amount of data of data blocks are judged as needing to be nullified, the judged data blocks of the target data recorded on the recording medium.

[0014]

With this construction, when a predetermined number of data blocks or a predetermined amount of data of data blocks satisfy a specific condition, the data blocks are sequentially nullified.

Accordingly, in cases such as where the target data can be used temporarily but cannot be copied or where the target data can be copied only one generation, generation of a copy is allowed despite copy prohibition, but instead the copy or the original is nullified. In this way, user-friendliness can be improved without departing from the principle of copy prohibition.

[0015]

Also, since the copy is nullified sequentially in units of the predetermined number of data blocks or the predetermined amount of data of data blocks, even if a malicious user tries to obtain the copy by powering off the device halfway through the operation, he or she can obtain only the predetermined number of data blocks or the predetermined amount of data of data blocks. By employing an appropriate unit of data for the nullification,

security can be improved.

[0016]

Description of the Preferred Embodiment(s)

(First Embodiment)

<Overview>

The first embodiment of the present invention relates to the following device. When digital content which is copy-prohibited is received, the device allows the digital content to be recorded onto a recording medium temporarily, but nullifies the recorded digital content once the recorded digital content has been reproduced or a predetermined time period has passed. This enables time-shifted viewing to be performed only for one viewing or only within the predetermined time period after the reception.

[0017]

<Construction>

FIG. 1 shows an example hardware construction of a reception/reproduction/nullification system to which the first embodiment of the present invention relates.

For purposes of explanation, FIG. 1 shows an antenna 901, a reception device 902, a monitor 903, a RAM 904, an HDD 905, a DVD recorder 906, and a ROM 907. A system LSI 800, the RAM 904, the HDD 905, and the ROM 907 are generally contained in the same case called an STB (set

top box).

[0018]

The system LSI 800 shown in FIG. 1 includes a transport stream decoder 801, an AV decoder 802, an encryption engine 803, and a microcomputer 804. These construction elements are enclosed within the same semiconductor chip, to prevent unencrypted digital data which is obtained by decoding a transport stream from being transferred over wiring of a circuit board. This strengthens security.

[0019]

The reception device 902 receives a desired carrier wave from a broadcast station via the antenna 901 and demodulates it, to produce a transport stream (hereafter a "TS stream") made up of packets storing control data and digital content to be used. If the digital content to be used requires copyright protection, information that indicates prohibition of copies is attached to the digital content. As one example, copy control information "Copy Never" is attached to the digital content. Furthermore, in the TS stream, a header unit including control information and the like is unencrypted, whereas a payload unit including data that need be transmitted is encrypted using a cipher called scrambling.

[0020]

The transport stream decoder 801 decrypts

(descrambles) the scrambled part of the TS stream generated by the reception device 902 using a decryption key which has been given to authorized users beforehand, and decodes the result. The transport stream decoder 801 also decodes the unscrambled part of the TS stream. Hence the transport stream decoder 801 obtains the digital content to be used. As one example, the digital content obtained here is an MPEG stream of audio and video.

[0021]

The AV decoder 802 generates a video output signal and an audio output signal from the digital content obtained by the transport stream decoder 801, and has the monitor 903 reproduce video and audio.

The encryption engine 803 operates as follows. If the digital content requires copyright protection and need be recorded to a recording medium such as the RAM 904, the HDD 905, or the DVD recorder 906, the encryption engine 803 encrypts the digital content obtained by the transport stream decoder 801 in units of a predetermined reproduction time period, using a randomly generated encryption key. The encryption engine 803 also encrypts a decryption key corresponding to the encryption key using a device ID, and records the encrypted digital content corresponding to the predetermined reproduction time period and the encrypted decryption key as a pair. To use the digital

content, the encryption engine 803 decrypts the encrypted decryption key using the device ID, and decrypts the encrypted digital content using the obtained decryption key. The device ID is a value which is unique to the semiconductor chip. In the present example, the device ID cannot be referred to from outside the semiconductor chip.

[0022]

The microcomputer 804 controls the overall operation of the STB, by reading a control program stored on the ROM 907 and executing it. Here, the control program has been scrambled to prevent unauthorized users from altering it, so that the microcomputer 804 descrambles the control program before executing it.

Suppose the user, who is viewing digital content accompanied by information that shows copy prohibition, indicates time-shifted viewing for some reason. Then the microcomputer 804 exercises control so that the following three operations are simultaneously carried out repeatedly: (1) recording encrypted digital content to the HDD 905; (2) decrypting encrypted digital content which was recorded onto the HDD 905 a shift time earlier, and reproducing the decrypted digital content; and (3) nullifying, in units of the predetermined reproduction time period, encrypted digital content on the HDD 905 which

has been reproduced so as to be no longer reproducible.

[0023]

Here, the encrypted digital content is nullified once it has been reproduced, but this condition for nullification may be replaced by or used in combination with the condition of whether a predetermined time period has passed since the time of recording. Most movie films run about two hours. Accordingly, if the predetermined time period is set at around 90 minutes, there is no moment at which the whole of the movie film is stored on a recording medium. As a result, even if the power is turned off halfway through the processing, the user cannot obtain the whole movie film in its entirety, and so cannot reproduce the whole movie film later. Hence time-shifted viewing can be performed only within the predetermined time period.

[0024]

FIG. 2 is a functional block diagram of a reception/reproduction/nullification device of the first embodiment of the present invention.

A reception/reproduction/nullification device 100 shown in FIG. 2 includes a user interface unit 101, a receiving unit 102, a descrambling unit 103, a key generating unit 104, a data encrypting unit 105, a key encrypting unit 106, a recording unit 107, a key decrypting unit 108, a data decrypting unit 109, a reproducing unit

110, a nullification judging unit 111, a processing capacity judging unit 112, a sequential nullifying unit 113, and a total nullifying unit 114. In actuality, the function of the receiving unit 102 corresponds to the function of the reception device 902 shown in FIG. 1. The function of the descrambling unit 103 corresponds to the function of the transport stream decoder 801 in FIG. 1. The functions of the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, the recording unit 107, the key decrypting unit 108, and the data decrypting unit 109 correspond to the function of the encryption engine 803 in FIG. 1. The function of the reproducing unit 110 corresponds to the function of the AV decoder 802 in FIG. 1. The functions of the nullification judging unit 111, the processing capacity judging unit 112, the sequential nullifying unit 113, and the total nullifying unit 114 correspond to the function of the microcomputer 804 in FIG. 1.

[0025]

It should be noted here that an explanation on functions which are not directly related to the present invention has been omitted in this specification for simplicity's sake, so that the following description may differ from the actual practice to some extent.

The user interface unit 101 receives various

indications from the user. The indications include a view indication, a pause indication, a time shift indication, a stop indication, and an indication to move digital content.

[0026]

The receiving unit 102 receives transmission data broadcast from a broadcast station or the like. In the present example, the receiving unit 102 receives digital content which has been scrambled and is accompanied with copy control information.

The descrambling unit 103 descrambles the scrambled digital content received by the receiving unit 102, using a decryption key which has been given to authorized users beforehand.

[0027]

The key generating unit 104 operates as follows. While the user is indicating a pause, the key generating unit 104 arbitrarily generates an arbitrary encryption key and a decryption key corresponding to the encryption key using a random number or the like, for each piece of digital content corresponding to a predetermined broadcast time period. Here, an algorithm that uses the same key for encryption and decryption is employed, so that an encryption key and a decryption key corresponding to the encryption key can be collectively referred to as a

generation key. For example, a generation key is randomly generated for each piece of digital content that corresponds to a broadcast time period of 10 minutes.

[0028]

The data encrypting unit 105 operates as follows. While the user is indicating a pause, the data encrypting unit 105 encrypts digital content descrambled by the descrambling unit 103 and corresponding to the predetermined broadcast time period, using an encryption key generated by the key generating unit 104, so that the encrypted digital content can be decrypted using a decryption key corresponding to the encryption key. In the present example, digital content corresponding to the broadcast time period of 10 minutes is encrypted using a corresponding generation key.

[0029]

The key encrypting unit 106 encrypts the decryption key corresponding to the encryption key used by the data encrypting unit 105, using the device ID. In the present example, the corresponding generation key is encrypted using the device ID.

The recording unit 107 records the digital content encrypted by the data encrypting unit 105 and corresponding to the predetermined broadcast time period and the corresponding decryption key encrypted by the key

encrypting unit 106, to a predetermined recording medium as a pair. In the present example, the pair of the digital content encrypted using the generation key and corresponding to the broadcast time period of 10 minutes and the encrypted generation key is recorded to the HDD. Here, if the digital content does not require copyright protection, the digital content may be recorded in an unencrypted form.

[0030]

The key decrypting unit 108 operates as follows. While the user is indicating time-shifted viewing, the key decrypting unit 108 reads an encrypted decryption key corresponding to digital content which is to be reproduced, from the recording medium. The key decrypting unit 108 then decrypts the encrypted decryption key using the device ID. In the present example, an encrypted generation key that is paired with digital content which was a shift time earlier (hereafter a "shift-time-old digital content") is decrypted.

The data decrypting unit 109 operates as follows. While the user is indicating time-shifted viewing, the data decrypting unit 109 decrypts digital content to be reproduced, using a decryption key decrypted by the key decrypting unit 108. In the present example, shift-time-old digital content is decrypted using a

decrypted generation key.

[0031]

The reproducing unit 110 operates as follows. While the user is indicating viewing, the reproducing unit 110 reproduces digital content descrambled by the descrambling unit 103. While the user is indicating time-shifted viewing, the reproducing unit 110 reproduces digital content decrypted by the data decrypting unit 109.

The nullification judging unit 111 operates as follows. When digital content is received and temporarily recorded despite its copy prohibition status, the nullification judging unit 111 judges, for each pair recorded on the recording medium and corresponding to the predetermined broadcast time period, whether the pair should be nullified, based on a specific condition. In the present example, the nullification judging unit 111 judges, for each pair of encrypted digital content corresponding to the broadcast time period of 10 minutes and an encrypted generation key, whether the pair should be nullified.

[0032]

The specific condition for nullification employed by the nullification judging unit 111 here is whether the digital content has been reproduced by the reproducing unit 110, or whether a predetermined time period has passed

from the time of reception by the receiving unit 102 or the time of recording by the recording unit 107. In the case where the lapse of the predetermined time period is used as the condition for nullification, the recording unit 107 further records time limit information that shows the reception time or recording time of digital content corresponding to the predetermined broadcast time period, in order to manage the recording time limit of the digital content. The nullification judging unit 111 judges whether the recording time limit is reached, according to this time limit information.

[0033]

The processing capacity judging unit 112 judges whether the device 100 has an enough processing capacity to destroy all data which is relating to digital content and is judged as needing to be nullified.

The sequential nullifying unit 113 operates as follows. When the nullification judging unit 111 judges that a predetermined number of pieces of digital content or a predetermined amount of data of pieces of digital content and their corresponding decryption keys should be nullified, the sequential nullifying unit 113 sequentially nullifies the parts that are judged as needing to be nullified, in a recording order.

[0034]

The nullification by the sequential nullifying unit 113 referred to here means to make data on the recording medium unusable. Ordinary data deletion merely deletes link information of a data file or rewrites several bits of the header unit of a data file, so that the data unit of the data file remains as it is. This being so, the data can be recovered in some cases even after the deletion instruction. Such data deletion cannot be regarded as making the data unusable. Accordingly, the sequential nullifying unit 113 destroys the very data that is to be nullified, by writing arbitrary data to a recording area on the recording medium where the data is recorded, or by initializing the recording area.

[0035]

Here, the sequential nullifying unit 113 may sequentially destroy all parts of data that needs to be nullified. In reality, however, sequentially overwriting with arbitrary data of the same size as the data to be nullified may cause a problem to the processing capacity of the device itself.

For instance, during time-shifted viewing it is necessary to simultaneously perform the following two sequence of operations. The first sequence of operations is receiving, descrambling, encrypting, and recording broadcast digital content. The second sequence of

operations is reading, decrypting, and reproducing recorded digital content. This puts a heavy load on the control system, the recording medium, and the like. This being so, to further execute a heavy-load operation of sequentially overwriting with arbitrary data of the same size as the whole data to be nullified, it is necessary to increase the processing capacity of the device itself or to restrict other functions.

[0036]

However, the act of nullifying data itself does not contribute to the user convenience at all. For this reason, it is undesirable to increase the processing capacity which would cause an increase in cost, or to limit other functions.

Accordingly, the sequential nullifying unit 113 may destroy at least an important part of the data to be nullified. For example, the important part is data that is necessary to reproduce the remaining parts of the data to be nullified. In more detail, the important part is a decryption key, an I picture in MPEG data, or a first sector of an I picture in MPEG data.

[0037]

As an alternative, the sequential nullifying unit 113 may destroy all parts of the data to be nullified if the processing capacity judging unit 112 judges that there is an enough processing capacity, and destroy only the

important part of the data to be nullified if the processing capacity judging unit 112 judges that there is not an enough processing capacity.

The total nullifying unit 114 destroys, of the data that needs to be nullified, all remaining data not destroyed by the sequential nullifying unit 113, when the processing capacity judging unit 112 judges that there is an enough processing capacity. Also, when the user indicates to stop time-shifted viewing, the total nullifying unit 114 destroys all remaining data not destroyed by the sequential nullifying unit 113.

[0038]

<First Operation Example>

FIG. 3 shows an example operation of the reception/reproduction/nullification device of the first embodiment of the present invention.

The operation of sequential reproduction, recording, time shifting, and nullification of the present invention is explained below, with reference to FIG. 3.

[0039]

(1) In the stopped state, the user interface unit 101 waits for receiving the user's indication to view some program (S1).

(2) Upon receiving the view indication (S1:Yes), the sequential reproduction starts (S2).

The receiving unit 102 starts receiving transmission data of the program which the user wants to view. In the present example, scrambled digital content with copy control information "Copy Never" is received.

[0040]

The descrambling unit 103 starts descrambling the scrambled digital content received by the receiving unit 102.

The reproducing unit 110 starts reproducing the digital content descrambled by the descrambling unit 103.

(3) During the sequential reproduction, the user interface unit 101 waits for the user's indication to stop (S3).

[0041]

(4) Upon receiving the stop indication (S3:Yes), the operations of the receiving unit 102, the descrambling unit 103, and the reproducing unit 110 are stopped to end the sequential reproduction and return to the stopped state (S4).

(5) During the sequential reproduction, the user interface unit 101 waits for the user's indication to pause (S5).

[0042]

(6) Upon receiving the pause indication (S5:Yes), the recording starts (S6).

The key generating unit 104 randomly generates an encryption key and a decryption key corresponding to the encryption key using a random number or the like, for each piece of digital content corresponding to the predetermined broadcast time period. In the present example, a generation key is randomly generated for each piece of digital content corresponding to the broadcast time period of 10 minutes.

[0043]

The data encrypting unit 105 encrypts digital content descrambled by the descrambling unit 103 and corresponding to the predetermined broadcast time period, using the encryption key generated by the key generating unit 104, so that the encrypted digital content can be decrypted using the corresponding decryption key. In the present example, the digital content corresponding to the broadcast time period of 10 minutes is encrypted using the corresponding generation key.

[0044]

The key encrypting unit 106 encrypts the decryption key corresponding to the encryption key used by the data encrypting unit 105, using the device ID. In the present example, the corresponding generation key is encrypted using the device ID.

The recording unit 107 records the digital content

encrypted by the data encrypting unit 105 and corresponding to the predetermined broadcast time period and the corresponding decryption key encrypted by the key encrypting unit 106, to the recording medium. In the present example, the pair of the digital content encrypted using the generation key and corresponding to the broadcast time period of 10 minutes and the encrypted generation key is recorded to the HDD.

[0045]

The reproducing unit 110 stops the sequential reproduction of digital content.

(7) During the recording, the nullification judging unit 111 judges, for each pair of encrypted digital content and an encrypted decryption key recorded on the recording medium and corresponding to the predetermined broadcast time period, whether the recording time limit of the pair is reached. In the present example, the recording time limit is set at 90 minutes, so that once 90 minutes have passed since a pair corresponding to the broadcast time period of 10 minutes was recorded, the nullification judging unit 111 judges that the recording time limit of the pair is reached (S7).

[0046]

(8) When the recording time limit of the pair is reached, the sequential nullifying unit 113 writes arbitrary data

to a recording area where the encrypted decryption key of the pair is recorded, to nullify the data in the recording area. Here, if the processing capacity judging unit 112 judges that there is an enough processing capacity, the sequential nullifying unit 113 further writes arbitrary data over the encrypted digital content of the pair, to nullify the data in the recording area (S8).

[0047]

(9) During the recording, the user interface unit 101 waits for the user's indication to stop (S9).

(10) Upon receiving the stop indication (S9:Yes), the operations of the receiving unit 102, the descrambling unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, and the recording unit 107 are stopped to end the recording. The total nullifying unit 114 destroys all remaining data which has not been destroyed by the sequential nullifying unit 113, before returning to the stopped state (S10).

[0048]

(11) During the recording, the user interface unit 101 waits for the user's indication to perform time-shifted viewing (S11).

(12) Upon receiving the time shift indication (S11:Yes), the time shifting starts (S12).

The key decrypting unit 108 reads an encrypted

decryption key paired with shift-time-old digital content from the recording medium, and decrypts the encrypted decryption key using the device ID. In the present example, the shift time is 30 minutes, so that the decryption begins from an encrypted generation key which is paired with digital content that was recorded 30 to 20 minutes earlier. If the shift time is longer than the recording time limit, the shift-time-old digital content has already been nullified by the time the time-shifted viewing is started and so cannot be reproduced. In such a case, the shift time is set as the recording time limit to continue the operation.

[0049]

The data decrypting unit 109 decrypts the corresponding encrypted digital content using the decryption key decrypted by the key decrypting unit 108. In the present example, the decryption begins from the digital content that was recorded 30 to 20 minutes earlier, using the decrypted generation key.

The reproducing unit 110 reproduces the digital content decrypted by the data decrypting unit 109.

[0050]

(13) During the time shifting, the nullification judging unit 111 judges, for each pair of encrypted digital content and an encrypted decryption key recorded on the

recording medium and corresponding to the predetermined broadcast time period, whether the recording time limit of the pair is reached or whether the digital content has been reproduced by the reproducing unit 110. In the present example, the recording time limit is 90 minutes, so that the nullification judging unit 111 judges, for each pair corresponding to the broadcast time period of 10 minutes, whether 90 minutes have passed since the recording or whether the digital content has been reproduced (S13).

[0051]

(14) When the pair is judged as needing to be nullified, the sequential nullifying unit 113 writes arbitrary data to a recording area of the encrypted decryption key of the pair to be nullified, to nullify the data in the recording area. Here, if the processing capacity judging unit 112 judges that there is an enough processing capacity, the sequential nullifying unit 113 further writes arbitrary data over the encrypted digital content of the pair to be nullified, to nullify the data in the recording area (S14).

[0052]

(15) During the time shifting, the user interface unit 101 waits for the user's indication to stop (S15).

(16) Upon receiving the stop indication (S15:Yes), the operations of the receiving unit 102, the descrambling

unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, the recording unit 107, the key decrypting unit 108, the data decrypting unit 109, and the reproducing unit 110 are stopped to end the time shifting. The total nullifying unit 114 destroys all remaining data which has not been destroyed by the sequential nullifying unit 113, before returning to the stopped state (S16).

[0053]

(17) During the time shifting, the user interface unit 101 waits for the user's indication to pause (S17).

(18) Upon receiving the pause indication (S17:Yes), the operations of the key decrypting unit 108, the data decrypting unit 109, and the reproducing unit 110 are stopped, and the operation proceeds to the recording (S18).

[0054]

<Second Operation Example>

In the first operation example, the recording is not performed during the sequential reproduction. Instead, upon receiving the user's indication to pause, the sequential reproduction is stopped and the recording is commenced. In the second operation example, on the other hand, the recording is performed during the sequential reproduction, so as to make it possible to perform time-shifted viewing even if the user does not indicate

to pause. Moreover, an automatic pause cancel function is added in the second operation example. This function automatically cancels the pause when the pause time reaches an upper limit, and proceeds to the time shifting.

[0055]

FIG. 4 shows another example operation of the reception/reproduction/nullification device of the first embodiment of the present invention.

Here, it is assumed that digital content received by the receiving unit 102 is accompanied with information showing a recording time limit (Storage Time) and a reproduction time limit (View Time).

The recording time limit is a time period which begins when a pair is recorded and after which the retention of the pair on the recording medium is prohibited. The reproduction time limit is a time period which begins when a pair is first reproduced and after which viewing is prohibited. A pair whose recording time limit or reproduction time limit is reached is judged as needing to be nullified.

[0056]

The operation of sequential reproduction/recording, recording, time shifting, nullification, and automatic pause canceling of the present invention is explained below, by referring to FIG. 4. Note here that steps which are

the same as those in the first operation example are given the same step numbers.

(1) In the stopped state, the user interface unit 101 waits for the user's indication to view some program (S1).

[0057]

(2) Upon receiving the view indication (S1:Yes), the sequential reproduction/recording starts (S102).

The receiving unit 102 starts receiving transmission data of the program which the user wants to view. In the present example, scrambled digital content with copy control information "Copy Never" is received.

[0058]

The descrambling unit 103 starts descrambling the scrambled digital content received by the receiving unit 102.

The reproducing unit 110 starts reproducing the digital content descrambled by the descrambling unit 103.

The key generating unit 104 randomly generates an encryption key and a decryption key corresponding to the encryption key using a random number or the like, for each piece of digital content corresponding to the predetermined broadcast time period. In the present example, a generation key is randomly generated for each piece of digital content corresponding to the broadcast time period

of 10 minutes.

[0059]

The data encrypting unit 105 encrypts the digital content descrambled by the descrambling unit 103 and corresponding to the predetermined broadcast time period, using the encryption key generated by the key generating unit 104, so that the encrypted digital content can be decrypted using the corresponding decryption key. In the present example, the digital content corresponding to the broadcast time period of 10 minutes is encrypted using the corresponding generation key.

[0060]

The key encrypting unit 106 encrypts the decryption key corresponding to the encryption key used by the data encrypting unit 105, using the device ID. In the present example, the corresponding generation key is encrypted using the device ID.

The recording unit 107 records the digital content encrypted by the data encrypting unit 105 and corresponding to the predetermined broadcast time period and the corresponding decryption key encrypted by the key encrypting unit 106, to the recording medium. In the present example, the pair of the digital content encrypted using the generation key and corresponding to the broadcast time period of 10 minutes and the encrypted generation

key is recorded to the HDD.

[0061]

Here, the pair recorded on the recording medium is accompanied with the recording time limit and the reproduction time limit together with time limit information. When the digital content is first reproduced, the time at which the digital content is first reproduced is added to the time limit information.

(3) During the sequential reproduction/recording, the nullification judging unit 111 refers to time limit information to judge, for each pair of encrypted digital content and an encrypted decryption key recorded on the recording medium and corresponding to the predetermined broadcast time period, whether the recording time limit of the pair is reached. Also, the nullification judging unit 111 judges, for each pair which has been reproduced, whether the reproduction time limit of the pair is reached. In the present example, the recording time limit is set at 90 minutes after the recording, and the reproduction time limit is set at 60 minutes after the reproduction. This being so, when 90 minutes have passed since a pair corresponding to the broadcast time period of 10 minutes was recorded, the recording time limit of the pair is judged as being reached. Also, when 60 minutes have passed since the pair was first reproduced, the reproduction time limit

of the pair is judged as being reached (S103).

[0062]

(4) When there is any pair whose recording time limit or reproduction time limit is reached, the sequential nullifying unit 113 writes arbitrary data to a recording area of the encrypted decryption key of the pair, to nullify the data in the recording area. Here, if the processing capacity judging unit 112 judges that there is an enough processing capacity, the sequential nullifying unit 113 further writes arbitrary data over the encrypted digital content of the pair, to nullify the data in the recording area (S104).

[0063]

(5) During the sequential reproduction/recording, the user interface unit 101 waits for the user's indication to stop (S105).

(6) Upon receiving the stop indication (S105:Yes), the operations of the receiving unit 102, the descrambling unit 103, the reproducing unit 110, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, and the recording unit 107 are stopped to end the sequential reproduction/recording. The total nullifying unit 114 destroys all remaining data which has not been destroyed by the sequential nullifying unit 113, before returning to the stopped state (S106).

[0064]

(7) During the sequential reproduction/recording, the user interface unit 101 waits for the user's indication to perform time-shifted viewing (S107).

(8) During the sequential reproduction/recording, the user interface unit 101 waits for the user's indication to pause (S108).

(9) Upon receiving the pause indication (S108:Yes), the reproduction is stopped while the recording continues (S109).

[0065]

The reproducing unit 110 stops the sequential reproduction of digital content.

(10) During the recording, the nullification judging unit 111 refers to time limit information to judge, for each pair of encrypted digital content and an encrypted decryption key recorded on the recording medium and corresponding to the predetermined broadcast time period, whether the recording time limit of the pair is reached. Also, the nullification judging unit 111 judges, for each pair which has been reproduced, whether the reproduction time limit of the pair is reached (S110).

[0066]

(11) When there is any pair whose recording time limit or reproduction time limit is reached, the sequential

nullifying unit 113 writes arbitrary data to a recording area of the encrypted decryption key of the pair, to nullify the data in the recording area. Here, if the processing capacity judging unit 112 judges that there is an enough processing capacity, the sequential nullifying unit 113 further writes arbitrary data over the encrypted digital content of the pair, to nullify the data in the recording area (S111).

[0067]

(12) During the recording, the user interface unit 101 waits for the user's indication to stop (S9).

(13) Upon receiving the stop indication (S9:Yes), the operations of the receiving unit 102, the descrambling unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, and the recording unit 107 are stopped to end the recording. The total nullifying unit 114 destroys all remaining data which has not been destroyed by the sequential nullifying unit 113, before returning to the stopped state (S10).

[0068]

(14) During the recording, the user interface unit 101 waits for the user's indication to perform time-shifted viewing (S11).

(15) During the recording, the sequential nullifying unit 113 judges whether the shift time reaches an upper

limit. If the shift time reaches the upper limit, the sequential nullifying unit 113 sets the shift time as the upper limit and automatically cancels the pause, so that the time shifting is commenced (S115). In the present example, the upper limit is set at 90 minutes which are the same as the recording time limit. In this way, even if the recording time limit is reached, any data will not be nullified without being reproduced once.

[0069]

(16) When the automatic pause canceling occurs (S115:Yes) or when the time shift indication is received (S107:Yes, S11:Yes), the time shifting starts (S116).

The key decrypting unit 108 reads an encrypted decryption key paired with shift-time-old digital content from the recording medium, and decrypts the encrypted decryption key using the device ID. In the present example, the shift time is 30 minutes, so that the decryption begins from an encrypted generation key paired with digital content which was recorded 30 to 20 minutes earlier. Here, if the shift time exceeds the recording time limit, the shift-time-old digital content has already been nullified by the time the time shifting starts and so cannot be reproduced. In this case, the shift time is set as the recording time limit to continue the operation.

[0070]

The data decrypting unit 109 decrypts the corresponding encrypted digital content using the decryption key decrypted by the key decrypting unit 108. In the present example, the decryption begins from the encrypted digital content of 30 to 20 minutes earlier, using the decrypted generation key.

The reproducing unit 110 reproduces the digital content decrypted by the data decrypting unit 109.

[0071]

(17) During the time shifting, the nullification judging unit 111 refers to time limit information to judge, for each pair of encrypted digital content and an encrypted decryption key recorded on the recording medium and corresponding to the predetermined broadcast time period, whether the recording time limit of the pair is reached. Also, the nullification judging unit 111 judges, for each pair which has been reproduced, whether the reproduction time limit of the pair is reached (S117).

[0072]

(18) When there is any pair whose recording time limit or reproduction time limit is reached, the sequential nullifying unit 113 writes arbitrary data to a recording area of the encrypted decryption key of the pair, to nullify the data in the recording area. Here, if the processing capacity judging unit 112 judges that there is an enough

processing capacity, the sequential nullifying unit 113 further writes arbitrary data over the encrypted digital content of the pair, to nullify the data in the recording area (S118).

[0073]

(19) During the time shifting, the user interface unit 101 waits for the user's indication to stop (S15).

(20) Upon receiving the stop indication (S15:Yes), the operations of the receiving unit 102, the descrambling unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, the recording unit 107, the key decrypting unit 108, the data decrypting unit 109, and the reproducing unit 110 are stopped to end the time shifting. The total nullifying unit 114 destroys all remaining data which has not been destroyed by the sequential nullifying unit 113, before returning to the stopped state (S16).

[0074]

(21) During the time shifting, the user interface unit 101 waits for the user's indication to pause (S17).

(22) Upon receiving the pause indication (S17:Yes), the operations of the key decrypting unit 108, the data decrypting unit 109, and the reproducing unit 110 are stopped, and the operation proceeds to the recording (S18).

[0075]

According to the first embodiment of the present invention, copy-prohibited digital content can be temporarily recorded to allow for time-shifted viewing, but the recorded data is promptly nullified. This allows user-friendliness to be improved without departing from the principle of copy prohibition.

(Second Embodiment)

<Overview>

The second embodiment of the present invention relates to the following device. When digital content which is copy-prohibited is received, the device allows the digital content to be temporarily recorded, but nullifies the recorded digital content once a predetermined time period has passed. Here, by writing new digital content to a recording area where old digital content which need be nullified has been stored, the old digital content which has been stored for more than the predetermined time period can be nullified without affecting the processing capacity of the device. As a result, time-shifted viewing can be performed only within the predetermined time period from the reception.

[0076]

<Construction>

A reception/reproduction/nullification device of

the second embodiment of the present invention has the same hardware construction as that of the first embodiment.

FIG. 5 is a functional block diagram of the reception/reproduction/nullification device of the second embodiment of the present invention.

[0077]

A reception/reproduction/nullification device 200 shown in FIG. 5 includes the user interface unit 101, the receiving unit 102, the descrambling unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, a recording unit 201, the key decrypting unit 108, the data decrypting unit 109, the reproducing unit 110, a nullification judging unit 202, the processing capacity judging unit 112, a sequential nullifying unit 203, and a total nullifying unit 204. In actuality, the function of the receiving unit 102 corresponds to the function of the reception device 902 shown in FIG. 1. The function of the descrambling unit 103 corresponds to the function of the transport stream decoder 801 in FIG. 1. The functions of the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, the recording unit 201, the key decrypting unit 108, and the data decrypting unit 109 correspond to the function of the encryption engine 803 in FIG. 1. The function of the reproducing unit 110 corresponds to the

function of the AV decoder 802 in FIG. 1. The functions of the nullification judging unit 202, the processing capacity judging unit 112, the sequential nullifying unit 203, and the total nullifying unit 204 correspond to the function of the microcomputer 804 in FIG. 1.

[0078]

Construction elements which are the same as those in the first embodiment are given the same reference numerals and their explanation has been omitted.

The recording unit 201 sequentially records pairs of digital content encrypted by the data encrypting unit 105 and corresponding to the predetermined broadcast time period and a corresponding decryption key encrypted by the key encrypting unit 106, onto the predetermined recording medium. Here, if the digital content is copy-prohibited, the recording unit 201 reserves a plurality of recording areas that are each capable of storing data of the predetermined broadcast time period, on the recording medium. The recording unit 201 then sequentially records the pairs to the reserved recording areas. In the present example, the recording unit 201 reserves nine recording areas that can each store data corresponding to the broadcast time period of 10 minutes, on the HDD. The recording unit 201 then records pairs of digital content encrypted using a generation key and

corresponding to the broadcast time period of 10 minutes and the encrypted generation key, sequentially to the reserved recording areas. Here, if the recording areas already store pairs, the recording unit 201 writes the new pairs over the old pairs. If the digital content does not require copyright protection, on the other hand, the recording unit 201 can record the digital content in an unencrypted form.

[0079]

The nullification judging unit 202 operates as follows. When digital content is received and temporarily recorded despite the copying being prohibited, the nullification judging unit 202 judges, for each pair recorded on the recording medium and corresponding to the predetermined broadcast time period, whether the pair should be nullified, based on a specific condition. In the present example, the nullification judging unit 202 judges, for each pair of encrypted digital content corresponding to the broadcast time period of 10 minutes and an encrypted generation key, whether the pair should be nullified.

[0080]

The specific condition for nullification employed by the nullification judging unit 202 is whether the digital content has been reproduced by the reproducing unit 110

or whether a predetermined time period has passed since the reception by the receiving unit 102 or the recording by the recording unit 201. In this embodiment, sequence information showing a sequence in which pairs were recorded on the recording medium is stored on the recording medium. This being so, the nullification judging unit 202 judges each of the pairs to be nullified in an order of the recording sequence, and the recording unit 201 writes the new pairs to the recording areas storing the old pairs which are judged as needing to be nullified. In the present example, nine pairs each corresponding to the broadcast time period of 10 minutes, which are respectively recorded in the nine recording areas on the recording medium, are each nullified 90 minutes after it was written, as a result of overwriting with a new pair.

[0081]

The sequential nullifying unit 203 operates as follows. Whenever the nullification judging unit 202 judges that a predetermined number of pieces of digital content or a predetermined amount of data of pieces of digital content and their corresponding encrypted decryption keys should be nullified, the sequential nullifying unit 203 sequentially nullifies recorded parts that are judged as needing to be nullified. Here, if there are new pairs which need to be recorded, the old pairs

can be nullified at the same time as recording the new pairs, by overwriting. If there is no new pair, the sequential nullifying unit 203 destroys the very data to be nullified, by, for example, continuously overwriting with arbitrary data.

[0082]

Here, if the digital content has a fixed bit rate, i.e., the amount of data per unit time is constant, old data can completely be nullified by the overwriting with new data. However, if the digital content has a variable bit rate as in MPEG, old data may not be able to be completely nullified by the overwriting with new data.

[0083]

In such a case, the sequential nullifying unit 203 may destroy all of the data to be nullified, by writing meaningless data over remaining parts which have not been overwritten with the new data. As an alternative, the sequential nullifying unit 203 may destroy all of the data to be nullified if the processing capacity judging unit 112 judges that there is an enough processing capacity, and leave the remaining parts not nullified by the overwriting with the new data as they are if the processing capacity judging unit 112 judges that there is not an enough processing capacity.

[0084]

The total nullifying unit 204 destroys, of the data to be nullified, all remaining data which has not been destroyed by the sequential nullifying unit 203, when there is an enough processing capacity. Also, the total nullifying unit 204 destroys all remaining data which has not been destroyed, when the user indicates to stop time-shifted viewing.

<Operation>

FIG. 6 shows an example operation of the reception/reproduction/nullification device of the second embodiment of the present invention.

[0085]

The operation of sequential reproduction, recording, time shifting, and nullification of the present invention is explained below, by referring to FIG. 6. Note here that steps which are the same as those in the first embodiment are given the same step numbers and their explanation has been omitted.

(1)-(5) Same as (1)-(5) in FIG. 3 in the first embodiment (S1-S5).

(6) Upon receiving the pause indication (S5:Yes), the recording starts (S21).

[0086]

The key generating unit 104 randomly generates an encryption key and a decryption key corresponding to the

encryption key using a random number of the like, for each piece of digital content corresponding to the predetermined broadcast time period. In the present example, a generation key is randomly generated for each piece of digital content corresponding to the broadcast time period of 10 minutes.

The data encrypting unit 105 encrypts the digital content descrambled by the descrambling unit 103 and corresponding to the predetermined broadcast time period, using the encryption key generated by the key generating unit 104, so that the encrypted digital content can be decrypted by the corresponding decryption key. In the present example, the digital content corresponding to the broadcast time period of 10 minutes is encrypted using the corresponding generation key.

[0087]

The key encrypting unit 106 encrypts the decryption key corresponding to the encryption key used by the data encrypting unit 105, using the device ID. In the present example, the corresponding generation key is encrypted using the device ID.

The recording unit 201 reserves a plurality of recording areas which can each store data of the predetermined broadcast time period, on the recording medium. The recording unit 201 then sequentially records

pairs of digital content encrypted by the data encrypting unit 105 and corresponding to the predetermined broadcast time period and a corresponding decryption key encrypted by the key encrypting unit 106, to the reserved recording areas. In the present example, nine recording areas each capable of storing data corresponding to the broadcast time period of 10 minutes are reserved on the HDD, and pairs of digital content encrypted using a generation key and corresponding to the broadcast time period of 10 minutes and the encrypted generation key are sequentially recorded to the nine recording areas. Here, if the recording areas already store pairs, the data is overwritten by new data.

[0088]

The sequential nullifying unit 203 destroys all of the data to be nullified, by, for example, writing meaningless data over parts that have not been nullified by the overwriting with the new data.

The reproducing unit 110 stops the sequential reproduction of the digital content.

(7) Same as (9) in FIG. 3 in the first embodiment (S9).

(8) Upon receiving the stop indication (S9:Yes), the operations of the receiving unit 102, the descrambling unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, and the recording

unit 201 are stopped to end the recording. The total nullifying unit 204 destroys all data which remains undestroyed, before returning to the stopped state (S22).

(9)-(10) Same as (11)-(12) in FIG. 3 in the first embodiment (S11-S12).

(11) Same as (15) in FIG. 3 in the first embodiment (S15).

(12) Upon receiving the stop indication (S15:Yes), the operations of the receiving unit 102, the descrambling unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, the recording unit 201, the key decrypting unit 108, the data decrypting unit 109, and the reproducing unit 110 are stopped to end the time shifting. The total nullifying unit 204 destroys all data which remains undestroyed, before returning to the stopped state (S23).

(13)-(14) Same as (17)-(18) in FIG. 3 in the first embodiment (S17-S18).

[0089]

According to the second embodiment of the present invention, copy-prohibited digital content can be temporarily recorded to allow for time-shifted viewing, but the recorded digital content is nullified by overwriting with new data once a predetermined time period has passed. This enables user-friendliness to be improved

without departing from the principle of copy prohibition, because the sequential nullification is executed without increasing the load on the device.

[0090]

(Third Embodiment)

<Overview>

The third embodiment of the present invention relates to the following device. In the third embodiment, when digital content whose copying is permitted only once is received and recorded on a recording medium, the digital content can be moved to another recording medium, but the digital content on the original recording medium is nullified little by little upon being copied, so that the digital content will not remain on the original recording medium.

[0091]

<Construction>

A reception/reproduction/nullification device of the third embodiment of the present invention has the same hardware construction as that of the first embodiment, except for the following.

The microcomputer 804 newly includes the following functions.

When the user receives digital content only one generation copy of which is permitted and records it to

the HDD 905 in an encrypted form, the microcomputer 804 copies encrypted digital content recorded on the HDD 905 and at the same time nullifies encrypted digital content on the HDD 905 so as to be unreproducible, in units of the predetermined reproduction time period.

[0092]

FIG. 7 is a functional block diagram of the reception/reproduction/nullification device of the third embodiment of the present invention.

A reception/reproduction/nullification device 300 shown in FIG. 7 includes the user interface unit 101, the receiving unit 102, the descrambling unit 103, the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, the recording unit 107, the key decrypting unit 108, the data decrypting unit 109, the reproducing unit 110, a moving unit 301, a nullification judging unit 302, the processing capacity judging unit 112, the sequential nullifying unit 113, and the total nullifying unit 114. In actuality, the function of the receiving unit 102 corresponds to the function of the reception device 902 shown in FIG. 1. The function of the descrambling unit 103 corresponds to the function of the transport stream decoder 801 in FIG. 1. The functions of the key generating unit 104, the data encrypting unit 105, the key encrypting unit 106, the recording unit 107, the

key decrypting unit 108, and the data decrypting unit 109 correspond to the function of the encrypting engine 803 in FIG. 1. The function of the reproducing unit 110 corresponds to the function of the AV decoder 802 in FIG. 1. The functions of the moving unit 301, the nullification judging unit 302, the processing capacity judging unit 112, the sequential nullifying unit 113, and the total nullifying unit 114 correspond to the function of the microcomputer 804 in FIG. 1.

[0093]

Construction elements which are the same as those in the first embodiment are given the same reference numerals and their explanation has been omitted.

The moving unit 301 moves pairs which have been recorded on the recording medium, sequentially to another recording medium. The movement referred to here is an operation of (1) copying data from one recording medium to another recording medium and (2) rewriting data management information of the data on the original recording medium to show that the data has been deleted, without deleting the data itself on the original recording medium. In the present example, pairs recorded on the HDD are moved one by one to another recording medium.

[0094]

The nullification judging unit 302 operates as

follows. When digital content is recorded to one recording medium and then further recorded to another recording medium despite that only one generation copy of the digital content is permitted, the nullification judging unit 302 judges, for each pair, whether the pair should be nullified, based on a specific condition. In the present example, the nullification judging unit 302 judges, for each pair of encrypted digital content corresponding to the broadcast time period of 10 minutes and an encrypted generation key, whether the pair should be nullified.

[0095]

The specific condition for nullification employed by the nullification judging unit 302 is whether the pair has been moved by the moving unit 301.

<Operation>

FIG. 8 shows an example operation of the reception/reproduction/nullification device of the third embodiment of the present invention.

[0096]

The operation of movement and nullification of the present invention is explained below, by referring to FIG. 8.

Suppose scrambled digital content whose copy control information is "Copy one Generation" is received, and a plurality of pairs of encrypted digital content

corresponding to the predetermined broadcast time period and an encrypted generation key are recorded on the HDD with copy control information "Copy No more", by a similar operation as the first embodiment.

[0097]

(1) In the stopped state, the user interface unit 101 waits for the user's indication to move digital content (S31).

(2) Upon receiving the move indication (S31:Yes), the nullification judging unit 302 judges whether the digital content is copy-prohibited, by checking whether the copy control information "Copy No more" is attached to the pairs to be moved by the moving unit 301 (S32).

[0098]

(3) If the digital content is not copy-prohibited (S32:No), the moving unit 301 moves all pairs of the digital content to another recording medium (S33).

(4) If the digital content is copy-prohibited (S32:Yes), the moving unit 301 moves one pair of the digital content to another recording medium. In the present example, one pair corresponding to the broadcast time period of 10 minutes and recorded on the HDD is moved to another recording medium.

[0099]

(5) The nullification judging unit 302 judges whether

there is a predetermined number of pairs or a predetermined amount of data of pairs which have been moved by the moving unit 301 but have not been nullified yet (S35).

(6) If there is a predetermined number of pairs or a predetermined amount of data of pairs which have been moved but have not been nullified (S35:Yes), the sequential nullifying unit 113 nullifies recorded parts which are judged as needing to be nullified (S36).

[0100]

(7) It is judged whether all pairs of the digital content have been moved (S37).

(8) If all pairs have been moved (S37:Yes), the total nullifying unit 114 destroys, of the data to be nullified, all remaining data which has not been destroyed by the sequential nullifying unit 113 (S38).

[0101]

According to the third embodiment of the present invention, copy-prohibited digital content can be moved to another recording medium but the digital content recorded on the original recording medium is then promptly nullified. This enables user-friendliness to improve without departing from the principle of copy prohibition.

The first to third embodiments describe the case where a different encryption key is generated for each piece of digital content corresponding to the predetermined

broadcast time period and the digital content corresponding to the predetermined broadcast time period is encrypted using the generated encryption key. However, a plurality of consecutively recorded pieces of digital content may be encrypted using the same encryption key. Also, the predetermined broadcast time period is not limited to the above example but may be in any length. Furthermore, digital content which is recorded on the same recording medium may be encrypted using a single encryption key unique to that recording medium.

[0102]

The first to third embodiments describe the case where nullification of encrypted digital content may be performed by destroying only a corresponding decryption key. However, when the same encryption key is used for encrypting a plurality of pieces of digital content as mentioned above, if the decryption key common to the plurality of pieces of digital content is destroyed, the other pieces of digital content that use the same decryption key cannot be decrypted. In this case, the decryption key is not destroyed and instead part or whole of the data itself is destroyed. The decryption key can of course be destroyed after the pieces of digital content that use the same decryption key are all nullified.

[0103]

Also, since data is usually recorded and managed in the form of files, each pair corresponding to the predetermined broadcast time period in the first to third embodiments may be recorded as an individual file, or a pair corresponding to a larger broadcast time period or a plurality of consecutive pairs may be recorded as the same file. When each pair is recorded as an individual file, nullification can be performed in units of files. However, when a plurality of pairs are recorded as a single file, nullification needs to be performed for part of the file. In such a case, access to the nullified part should be restricted so as to keep the nullified part from being accessed by mistake. Access to part of a file can be restricted by, for example, using a seek restriction function of a file pointer mounted on a typical operating system.

[0104]

In the third embodiment, the plurality of recording areas reserved by the recording unit 201 on the recording medium need not be consecutive. As one example, AV data of 4Mbps is 300MB per ten minutes. It is not efficient to reserve consecutive recording areas that can store such an amount of data on the HDD. In this case, each recording area is made up of a plurality of small consecutive areas. The relationship between each recording area and its small

consecutive areas is independently managed by a file system, which provides each recording area to higher applications as a consecutive recording area to realize access using a file pointer.

[0105]

Programs that can execute the operations of the first to third embodiments on a computer may be recorded on computer-readable recording media and distributed for transaction. Such programs may also be distributed via a network or the like for transaction.

Examples of the computer-readable recording media include a removable recording medium such as a floppy disk, a CD, an MO, a DVD, or a memory card, and a fixed recording medium such as a hard disk and a semiconductor memory. There are no specific limitations on the types of the computer-readable recording media.

[0106]

Effects of the Invention

The data nullification device according to the present invention is a data nullification device for nullifying target data recorded on a recording medium, the target data being made up of a plurality of data blocks, the data nullification device being characterized by including: a judging unit operable to judge, for each data block recorded on the recording medium, whether the data

block needs to be nullified; and a nullifying unit operable to sequentially nullify, when a predetermined number of data blocks or a predetermined amount of data of data blocks are judged as needing to be nullified, the judged data blocks of the target data recorded on the recording medium.

[0107]

With this construction, when a predetermined number of data blocks or a predetermined amount of data of data blocks satisfy a specific condition, the data blocks are nullified.

Accordingly, when the target data can be temporarily used but cannot be copied, or when the target data can be copied only one generation, the generation of a prohibited copy is temporarily permitted but instead the copy or the original is reliably nullified. In this way, user-friendliness can be improved without departing from the principle of copy prohibition.

[0108]

Also, since the copy is nullified sequentially in units of a predetermined number of data blocks or a predetermined amount of data of data blocks, even if a malicious user tries to obtain the copy by powering off the device halfway through the operation, he or she can only obtain the predetermined number of data blocks or the predetermined amount of data of data blocks of the

copy. By employing an appropriate data unit for the nullification, security can be improved.

Here, in the data nullification device, the recording medium may store sequence information that shows a sequence in which the plurality of data blocks are recorded onto the recording medium, wherein the judging unit judges, in succession, the plurality of data blocks in the sequence shown by the sequence information, as needing to be nullified.

[0109]

With this construction, the plurality of data blocks are judged, in the recording sequence, as needing to be nullified.

This allows only a new data block to be retained on the recording medium, since a data block which was recorded earlier is nullified first.

Here, in the data nullification device, the target data recorded on the recording medium may be data which is continuously transmitted from an external device and recorded on the recording medium, wherein the data nullification device further includes: a receiving unit operable to receive data from the external device, and having set the received data as a new data block, the nullifying unit writes the new data block to a recording area, on the recording medium, that stores a data block

which is judged as needing to be nullified, to nullify the recorded data block and at the same time record the new data block.

[0110]

With this construction, the new data block is written to the recording area over the old data block which is judged as needing to be nullified.

In other words, recording the new data block has the effect of nullifying the old data block. Accordingly, the load on the device hardly increases despite the execution of the nullification.

Here, in the data nullification device, each data block may have a length corresponding to a fixed transmission time period, wherein a specified number of recording areas which are each used as a recording area of a data block are reserved on the recording medium.

[0111]

With this construction, the specified number of recording areas each for recording data of the fixed transmission time period is reserved on the recording medium.

Accordingly, the fixed recording time limit can be applied to each set of data.

Here, in the data nullification device, if the length corresponding to the fixed transmission time period is

variable and if part of the recorded data block remains even after the new data block is written, the nullifying unit may further write arbitrary data over the part of the recorded data block.

[0112]

With this construction, arbitrary data is written over parts which have not been destroyed by the overwriting with the new data block.

This makes it possible to completely destroy the data to be nullified.

Here, in the data nullification device, if there is not a new data block which is to be recorded, the nullifying unit may write arbitrary data to the recording area.

[0113]

With this construction, even when there is not a new data block, arbitrary data is written over continuously.

This enables each data block which was recorded earlier, to be completely destroyed.

Here, in the data nullification device, the recording medium may store time limit information showing a recording time limit of each data block recorded on the recording medium, the recording time limit being a time limit after which retention of the data block on the recording medium is prohibited, wherein the judging unit judges that each data block whose recording time limit is reached needs

to be nullified, based on the time limit information.

[0114]

With this construction, each data block whose recording time limit is reached is judged as needing to be nullified.

Since each data block is nullified based on its recording time limit, it is possible to make such settings that give priorities to data blocks. This increases flexibility.

Here, the data nullification device may further include: a utilizing unit operable to utilize the target data recorded on the recording medium, in units of data blocks, wherein the judging unit further judges that each data block which was utilized by the utilizing unit needs to be nullified.

[0115]

With this construction, each utilized data block is judged as needing to be nullified.

Since each utilized data block is nullified, user-friendliness can be improved without departing from the principle of copy prohibition.

Here, the data nullification device may further include: a utilizing unit operable to utilize the target data recorded on the recording medium, in units of data blocks, wherein the judging unit further judges that each

data block which was utilized by the utilizing unit needs to be nullified.

[0116]

With this construction, each utilized data block is judged as needing to be nullified.

Since each utilized data block is nullified, by nullifying each data block which was reproduced, copied, or moved, user-friendliness can be improved without departing from the principle of copy prohibition.

[0117]

Here, in the data nullification device, the target data recorded on the recording medium may be content data which is transmitted from an external device and recorded on the recording medium, wherein the content data is accompanied with copy control information showing whether copying of the content data is permitted or prohibited, the utilizing unit reproduces the content data recorded on the recording medium, in units of data blocks, and only if the copy control information accompanying the content data shows that the copying of the content data is prohibited, the judging unit judges that each data block which was reproduced by the utilizing unit needs to be nullified.

[0118]

With this construction, if the copy control information shows that the copying of the content data

is prohibited, a data block is judged as needing to be nullified.

In other words, when the content data is copy-prohibited, a copy of the content data is temporarily permitted but then the copy is reliably nullified.

Here, in the data nullification device, the target data recorded on the recording medium may be accompanied with copy control information showing whether copying of the target data is permitted or prohibited, wherein the utilizing unit records the target data recorded on the recording medium, to another recording medium, in units of data blocks, and only if the copy control information accompanying the target data shows that the copying of the target data is prohibited, the judging unit judges that each data block on the recording medium which corresponds to a data block recorded to the other recording medium by the utilizing unit needs to be nullified.

[0119]

With this construction, if the copy control information shows that the copying of the content data is prohibited, a data block is judged as needing to be nullified.

In other words, when the content data is copy-prohibited, a copy of the content data is temporarily permitted but then the original is reliably nullified.

Here, in the data nullification device, the nullifying unit may destroy all parts of a data block which is judged as needing to be nullified.

[0120]

With this construction, all parts of the data block judged as needing to be nullified are destroyed.

This enhances security.

Here, in the data nullification device, the nullifying unit may destroy at least a part of a data block which is judged as needing to be nullified, the part of the data block being necessary to utilize remaining parts of the data block.

[0121]

With this construction, at least the data which is needed to utilize the other data is destroyed.

This makes the data unusable while minimizing the increase in the load of the device.

Here, in the data nullification device, the target data recorded on the recording medium may be MPEG data including I pictures, wherein the part of the data block necessary to utilize the remaining parts of the data block is an I picture.

[0122]

With this construction, the data which is needed to utilize the other data is an I picture in MPEG data.

B pictures and P pictures cannot be utilized if the I picture which these B pictures and P pictures refer to is destroyed. By destroying only the I picture while leaving the B and P pictures as they are, the increase in the load of the device is reduced.

[0123]

Here, in the data nullification device, the target data recorded on the recording medium may be MPEG data including I pictures, wherein the part of the data block necessary to utilize the remaining parts of the data block is a first sector of an I picture.

With this construction, the data which is needed to utilize the other data is the first sector of the I picture.

[0124]

This makes it impossible to properly reproduce the I picture, so that the remaining B and P pictures cannot be reproduced. Thus, by destroying only the first sector of the I picture, the increase in the load of the device can be reduced.

Here, in the data nullification device, when the data nullification device does not have an enough processing capacity, the nullifying unit may destroy only the part of the data block necessary to utilize the remaining parts of the data block.

[0125]

With this construction, when there is not an enough processing capacity, only the data which is needed to utilize the other data is destroyed.

This enhances security without increasing the load of the device.

Here, in the data nullification device, the nullifying unit may destroy the remaining parts of the data block within a range where a processing capacity of the data nullification device allows.

[0126]

With this construction, the other data is destroyed within a range where the processing capacity of the device allows.

This enhances security without increasing the load of the device.

Here, the data nullification device may further include: a total destroying unit operable to destroy remaining parts of data blocks which were not destroyed by the nullifying unit, when the data nullification device has an enough processing capacity.

[0127]

With this construction, when there is an enough processing capacity, the remaining data not destroyed by the sequential nullifying unit is all destroyed.

This enhances security without increasing the load

of the device.

Here, in the data nullification device, each data block recorded on the recording medium may be encrypted using an individual data block encryption key, wherein a data block decryption key for decrypting the encrypted data block is stored on the recording medium, and the nullifying unit destroys at least a data block decryption key, on the recording medium, corresponding to a data block which is judged as needing to be nullified.

[0128]

With this construction, at least the data block decryption key corresponding to the data block is destroyed. As a result, the encrypted data block remaining on the recording medium becomes unusable, since the encrypted data block cannot be decrypted without the data block decryption key.

Thus, the data is made unusable with a minimum increase in the load of the device.

[0129]

Here, the data nullification device may further include: an acquiring unit operable to acquire the target data in an encrypted form; a decrypting unit operable to decrypt the encrypted target data using a user key which has been provided to authorized users in advance, to obtain the target data; a key generating unit operable to generate

an arbitrary data block encryption key and a data block decryption key corresponding to the data block encryption key, for each data block of the target data; a data encrypting unit operable to encrypt the data block using the data block encryption key so that the encrypted data block can be decrypted using the corresponding data block decryption key; a key encrypting unit operable to encrypt the data block decryption key using an identifier unique to the data nullification device; and a recording unit operable to record the encrypted data block and the encrypted data block decryption key onto the recording medium.

[0130]

With this construction, the encrypted target data is decrypted using the user key, and each data block of the decrypted target data is individually encrypted using a data block encryption key. Further, a data block decryption key corresponding to the data block encryption key is encrypted using an identifier unique to the device, and the encrypted data block and the encrypted data block decryption key are recorded onto the recording medium.

Since the recorded data cannot be decrypted without the identifier unique to the device and so cannot be used by other devices, the security can be enhanced.

[0131]

Here, in the data nullification device, at least the

decrypting unit, the key generating unit, the data encrypting unit, and the key encrypting unit may be contained in a single semiconductor chip.

With this construction, the decrypting unit, the key generating unit, the data encrypting unit, and the key encrypting unit can be contained in the same semiconductor chip. This keeps the target data in an unencrypted form from being transferred over wiring of a circuit board.

[0132]

In other words, an unauthorized user cannot retrieve the unencrypted target data during the operation. This enhances the security.

The data nullification program according to the present invention is a data nullification program for nullifying target data recorded on a recording medium, the target data being made up of a plurality of data blocks, the data nullification program being characterized by having a computer execute: a judging step of judging, for each data block recorded on the recording medium, whether the data block needs to be nullified; and a nullifying step of sequentially nullifying, when a predetermined number of data blocks or a predetermined amount of data of data blocks are judged as needing to be nullified, the judged data blocks.

[0133]

With this construction, when a predetermined number of data blocks or a predetermined amount of data of data blocks satisfy a specific condition, the data blocks are nullified.

Accordingly, when the target data is copy-prohibited though it can be temporarily used or when the target data can be copied only one generation, the generation of a prohibited copy is temporarily permitted but instead the copy or the original is reliably nullified. In this way, the user-friendliness can be improved without departing from the principle of copy prohibition.

[0134]

Also, since the copy is nullified sequentially in units of a predetermined number of data blocks or a predetermined amount of data of data blocks, even if a malicious user tries to obtain the copy by powering off the device halfway through the operation, he or she can only obtain the predetermined number of data blocks or the predetermined amount of data of data blocks of the copy. By employing an appropriate data unit for the nullification, the security can be improved.

Here, in the data nullification program, the recording medium may store sequence information that shows a sequence in which the plurality of data blocks are recorded onto the recording medium, wherein the judging step judges,

in succession, the plurality of data blocks in the sequence shown by the sequence information, as needing to be nullified.

[0135]

With this construction, the plurality of data blocks are judged, in the recording sequence, as needing to be nullified.

This allows only a new data block to be retained on the recording medium, since a data block which was recorded earlier is nullified first.

Here, in the data nullification program, the target data recorded on the recording medium may be data which is continuously transmitted from an external device and recorded on the recording medium, wherein the data nullification program further having the computer execute: a receiving step of receiving data from the external device, and having set the received data as a new data block, the nullifying step writes the new data block to a recording area, on the recording medium, that stores a data block which is judged as needing to be nullified, to nullify the recorded data block and at the same time record the new data block.

[0136]

With this construction, the new data block is written to the recording area over the old data block which is

judged as needing to be nullified.

In other words, recording the new data block has the effect of nullifying the old data block. Accordingly, the load on the device hardly increases despite the execution of the nullification.

Here, in the data nullification program, the recording medium may store time limit information showing a recording time limit of each data block recorded on the recording medium, the recording time limit being a time limit after which retention of the data block on the recording medium is prohibited, wherein the judging step judges that each data block whose recording time limit is reached needs to be nullified, based on the time limit information.

[0137]

With this construction, each data block whose recording time limit is reached is judged as needing to be nullified.

Since each data block is nullified based on its recording time limit, it is possible to make such settings that give a priority to each data block. This increases flexibility.

Here, the data nullification program may further have the computer execute: a utilizing step of utilizing the target data recorded on the recording medium, in units

of data blocks, wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

[0138]

With this construction, each utilized data block is judged as needing to be nullified.

This improves user-friendliness without departing from the principle of copy prohibition, since each utilized data block is nullified.

Here, the data nullification program may further have the computer execute: a utilizing step of utilizing the target data recorded on the recording medium, in units of data blocks, wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

[0139]

With this construction, each utilized data block is judged as needing to be nullified.

Since each utilized data block is nullified, by nullifying each data block which was reproduced, copied, or moved, user-friendliness can be improved without departing from the principle of copy prohibition.

[0140]

Here, in the data nullification program, the nullifying step may destroy all parts of a data block which

is judged as needing to be nullified.

With this construction, all parts of the data block judged as needing to be nullified are destroyed.

[0141]

This enhances security.

Here, in the data nullification program, the nullifying step may destroy at least a part of a data block which is judged as needing to be nullified, the part of the data block being necessary to utilize remaining parts of the data block.

[0142]

With this construction, at least the data which is needed to utilize the other data is destroyed.

This makes the data unusable while minimizing the increase in the load of the device.

Here, in the data nullification program, each data block recorded on the recording medium may be encrypted using an individual data block encryption key, wherein a data block decryption key for decrypting the encrypted data block is stored on the recording medium, and the nullifying step destroys at least a data block decryption key, on the recording medium, corresponding to a data block which is judged as needing to be nullified.

[0143]

With this construction, at least the data block

decryption key is destroyed. As a result, the data block remaining on the recording medium becomes unusable, since the data block cannot be decrypted without the data block decryption key.

Thus, the data is made unusable with a minimum increase in the load of the device.

[0144]

The data nullification method according to the present invention is a data nullification method for nullifying target data recorded on a recording medium, the target data being made up of a plurality of data blocks, the data nullification method being characterized by including: a judging step of judging, for each data block recorded on the recording medium, whether the data block needs to be nullified; and a nullifying step of sequentially nullifying, when a predetermined number of data blocks or a predetermined amount of data of data blocks are judged as needing to be nullified, the judged data blocks.

[0145]

With this construction, when a predetermined number of data blocks or a predetermined amount of data of data blocks satisfy a specific condition, the data blocks are nullified.

Accordingly, when the target data is copy-prohibited though it can be used temporarily or when the target data

can be copied only one generation, the generation of a prohibited copy is temporarily permitted but then the copy or the original is reliably nullified. In this way, user-friendliness can be improved without departing from the principle of copy prohibition.

[0146]

Also, since the copy is nullified in units of the predetermined number of data blocks or the predetermined amount of data of data blocks, even if a malicious user tries to obtain the copy by powering off the device halfway through the operation, he or she can only obtain the predetermined number of data blocks or the predetermined amount of data of data blocks of the copy. By employing an appropriate data unit for the nullification, security can be improved.

Here, in the data nullification method, the recording medium may store sequence information that shows a sequence in which the plurality of data blocks are recorded onto the recording medium, wherein the judging step judges, in succession, the plurality of data blocks in the sequence shown by the sequence information, as needing to be nullified.

[0147]

With this construction, the plurality of data blocks are judged, in the recording sequence, as needing to be

nullified.

This allows only a new data block to be retained on the recording medium, since a data block which was recorded earlier is nullified first.

Here, in the data nullification method, the target data recorded on the recording medium may be data which is continuously transmitted from an external device and recorded on the recording medium, wherein the data nullification method further includes: a receiving step of receiving data from the external device, and having set the received data as a new data block, the nullifying step writes the new data block to a recording area, on the recording medium, that stores a data block which is judged as needing to be nullified, to nullify the recorded data block and at the same time record the new data block. [0148]

With this construction, the new data block is written to the recording area over the old data block which is judged as needing to be nullified.

In other words, recording the new data block has the effect of nullifying the old data block. Accordingly, the load on the device hardly increases despite the execution of the nullification.

Here, in the data nullification method, the recording medium may store time limit information showing a recording

time limit of each data block recorded on the recording medium, the recording time limit being a time limit after which retention of the data block on the recording medium is prohibited, wherein the judging step judges that each data block whose recording time limit is reached needs to be nullified, based on the time limit information.

[0149]

With this construction, each data block whose recording time limit is reached is judged as needing to be nullified.

Since each data block is nullified based on its recording time limit, it is possible to make such settings that give a priority to each data block. This increases flexibility.

Here, the data nullification method may further include: a utilizing step of utilizing the target data recorded on the recording medium, in units of data blocks, wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

[0150]

With this construction, each utilized data block is judged as needing to be nullified.

Since each utilized data block is nullified, user-friendliness can be improved without departing from

the principle of copy prohibition.

Here, the data nullification method may further include: a utilizing step of utilizing the target data recorded on the recording medium, in units of data blocks, wherein the judging step further judges that each data block which was utilized in the utilizing step needs to be nullified.

[0151]

With this construction, each utilized data block is judged as needing to be nullified.

Since each utilized data block is nullified, by nullifying each data block which was reproduced, copied, or moved, user-friendliness can be improved without departing from the principle of copy prohibition.

[0152]

Here, in the data nullification method, the nullifying step may destroy all parts of a data block which is judged as needing to be nullified.

With this construction, all parts of the data block judged as needing to be nullified are destroyed.

[0153]

This enhances security.

Here, in the data nullification method, the nullifying step may destroy at least a part of a data block which is judged as needing to be nullified, the part of

the data block being necessary to utilize remaining parts of the data block.

[0154]

With this construction, at least the data which is needed to utilize the other data is destroyed.

This makes the data unusable while minimizing the increase in the load of the device.

Here, in the data nullification method, each data block recorded on the recording medium may be encrypted using an individual data block encryption key, wherein a data block decryption key for decrypting the encrypted data block is stored on the recording medium, and the nullifying step destroys at least a data block decryption key, on the recording medium, corresponding to a data block which is judged as needing to be nullified.

[0155]

With this construction, at least the data block decryption key is destroyed. As a result, the data block remaining on the recording medium becomes unusable, since the data block cannot be decrypted without the data block decryption key.

Thus, the data is made unusable with a minimum increase in the load of the device.

Simplified Description of the Drawings

FIG. 1 shows an example hardware construction of a reception/reproduction/nullification device to which the first embodiment of the present invention relates.

FIG. 2 is a functional block diagram of the reception/reproduction/nullification device to which the first embodiment of the present invention relates.

FIG. 3 shows an example operation of the reception/reproduction/nullification device to which the first embodiment of the present invention relates.

FIG. 4 shows another example operation of the reception/reproduction/nullification device to which the first embodiment of the present invention relates.

FIG. 5 is a functional block diagram of a reception/reproduction/nullification device to which the second embodiment of the present invention relates.

FIG. 6 shows an example operation of the reception/reproduction/nullification device to which the second embodiment of the present invention relates.

FIG. 7 is a functional block diagram of a reception/reproduction/nullification device to which the third embodiment of the present invention relates.

FIG. 8 shows an example operation of the reception/reproduction/nullification device to which the third embodiment of the present invention relates.

Numerical References

100 .... reception/reproduction/nullification device

101 .... user interface unit

102 .... receiving unit

103 .... descrambling unit

104 .... key generating unit

105 .... data encrypting unit

106 .... key encrypting unit

107 .... recording unit

108 .... key decrypting unit

109 .... data decrypting unit

110 .... reproducing unit

111 .... nullification judging unit

112 .... processing capacity judging unit

113 .... sequential nullifying unit

114 .... total nullifying unit

200 .... reception/reproduction/nullification device

201 .... recording unit

202 .... nullification judging unit

203 .... sequential nullifying unit

204 .... total nullifying unit

300 .... reception/reproduction/nullification device

301 .... moving unit

302 .... nullification judging unit

800 .... system LSI

801 .... transport stream decoder

802 .... AV decoder

803 .... encryption engine

804 .... microcomputer

ABSTRACT OF THE DISCLOSURE

Problem

To provide a data nullification device for improving user-friendliness without departing from the principle of copy prohibition.

Solution

The data nullification device includes: a receiving unit 102 for receiving data which is copy-prohibited; a recording unit 107 for recording the received data in units of data blocks; a reproducing unit 110 for sequentially reproducing the recorded data blocks; a nullification judging unit 111 for judging that a data block needs to be nullified when a recording time limit of the data block is reached, the data block is reproduced, and the like; and a sequential nullifying unit 113 for destroying, in the data block to be nullified, at least data that is needed to utilize other data, by overwriting with new data or arbitrary data.

Selected Drawing FIG. 2

FIG. 1

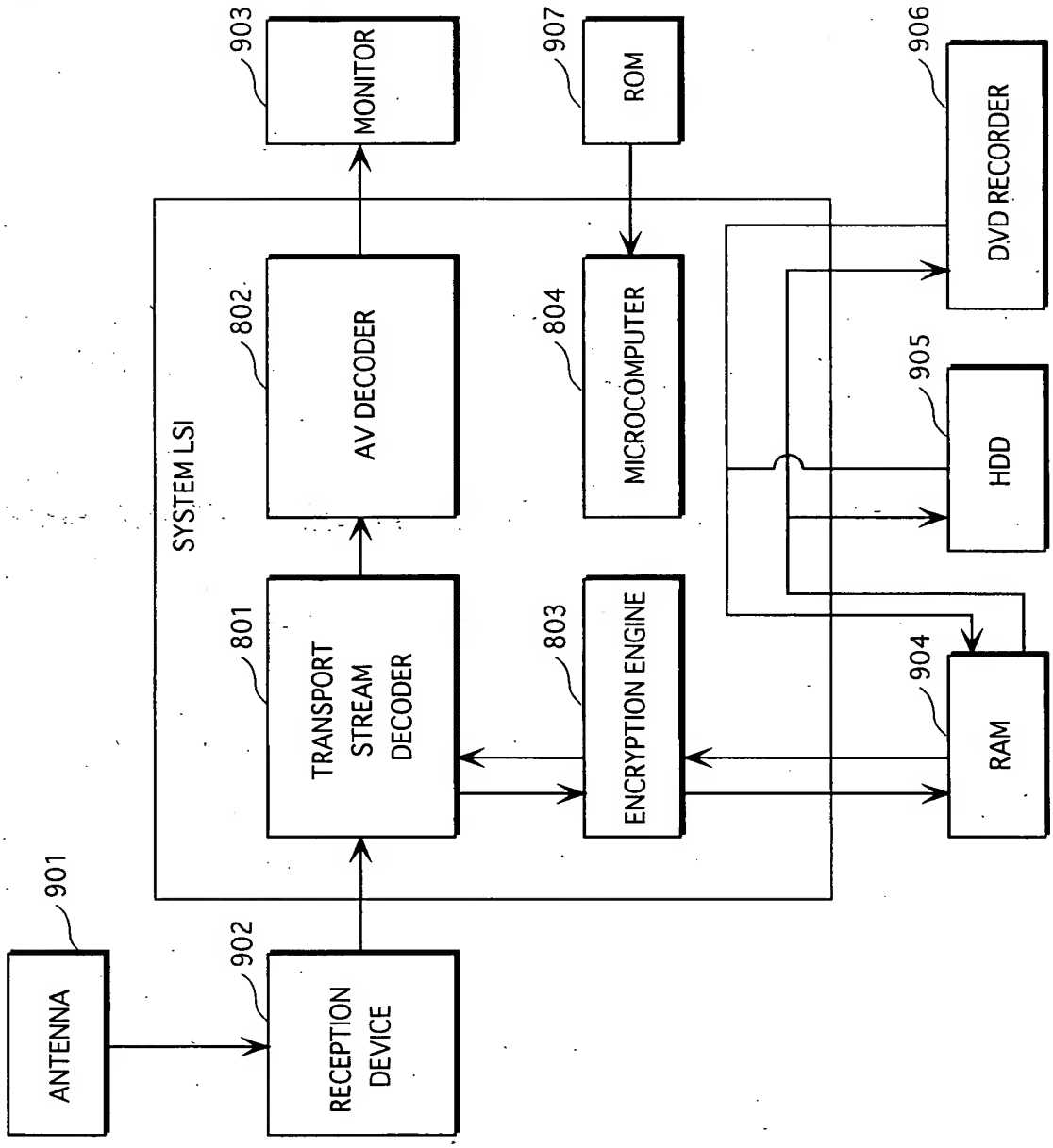


FIG. 2

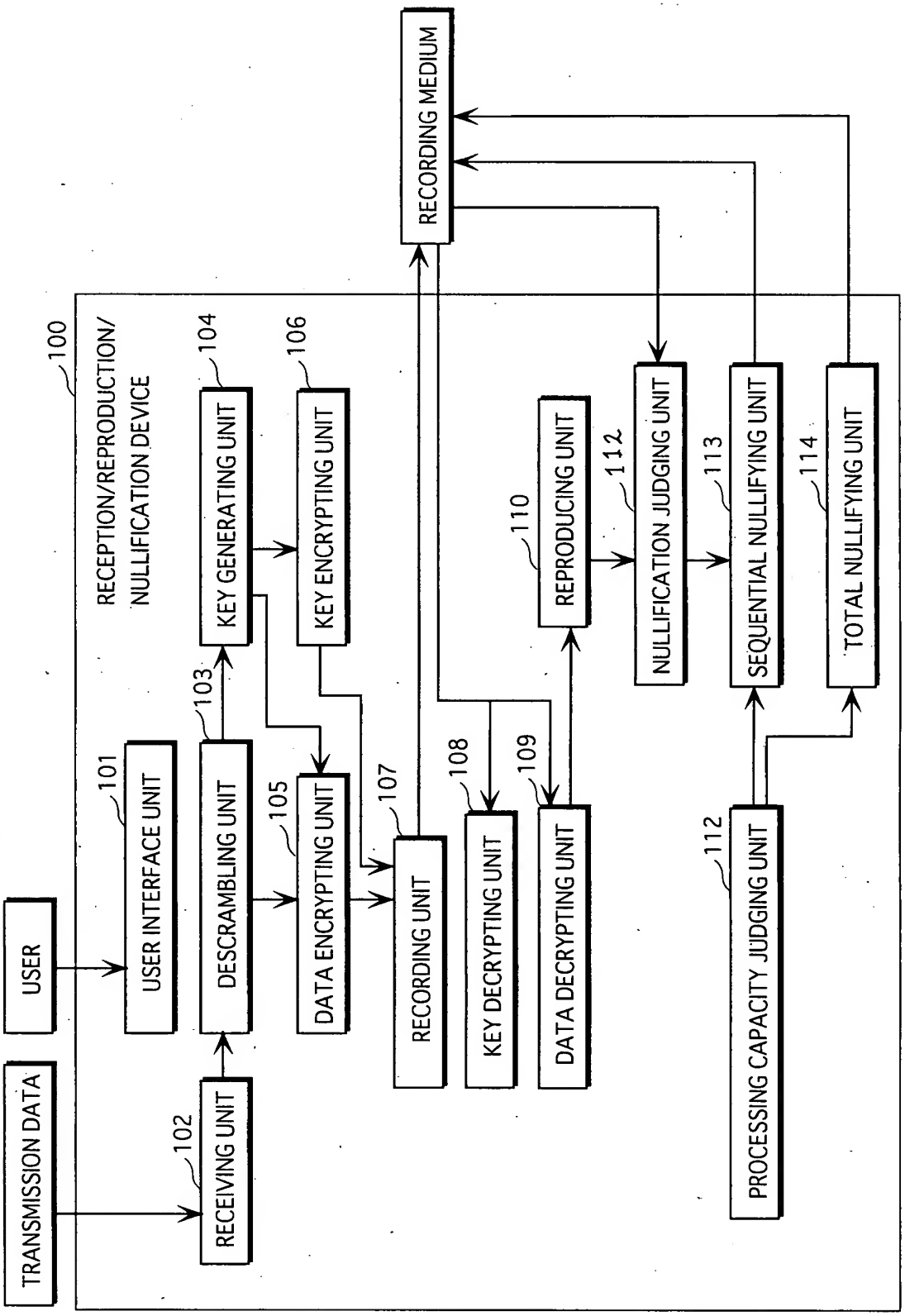

RECORDING MEDIUM
100
RECEPTION/REPRODUCTION/
NULLIFICATION DEVICE
104
KEY GENERATING UNIT
106
KEY ENCRYPTING UNIT
110
REPRODUCING UNIT
112
NULLIFICATION JUDGING UNIT
113
SEQUENTIAL NULLIFYING UNIT
114
TOTAL NULLIFYING UNIT
103
101
USER INTERFACE UNIT
DESCRAMBLING UNIT
105
DATA ENCRYPTING UNIT
107
RECORDING UNIT
108
KEY DECRYPTING UNIT
109
DATA DECRYPTING UNIT
112
PROCESSING CAPACITY JUDGING UNIT
USER
TRANSMISSION DATA
102
RECEIVING UNIT

FIG.3

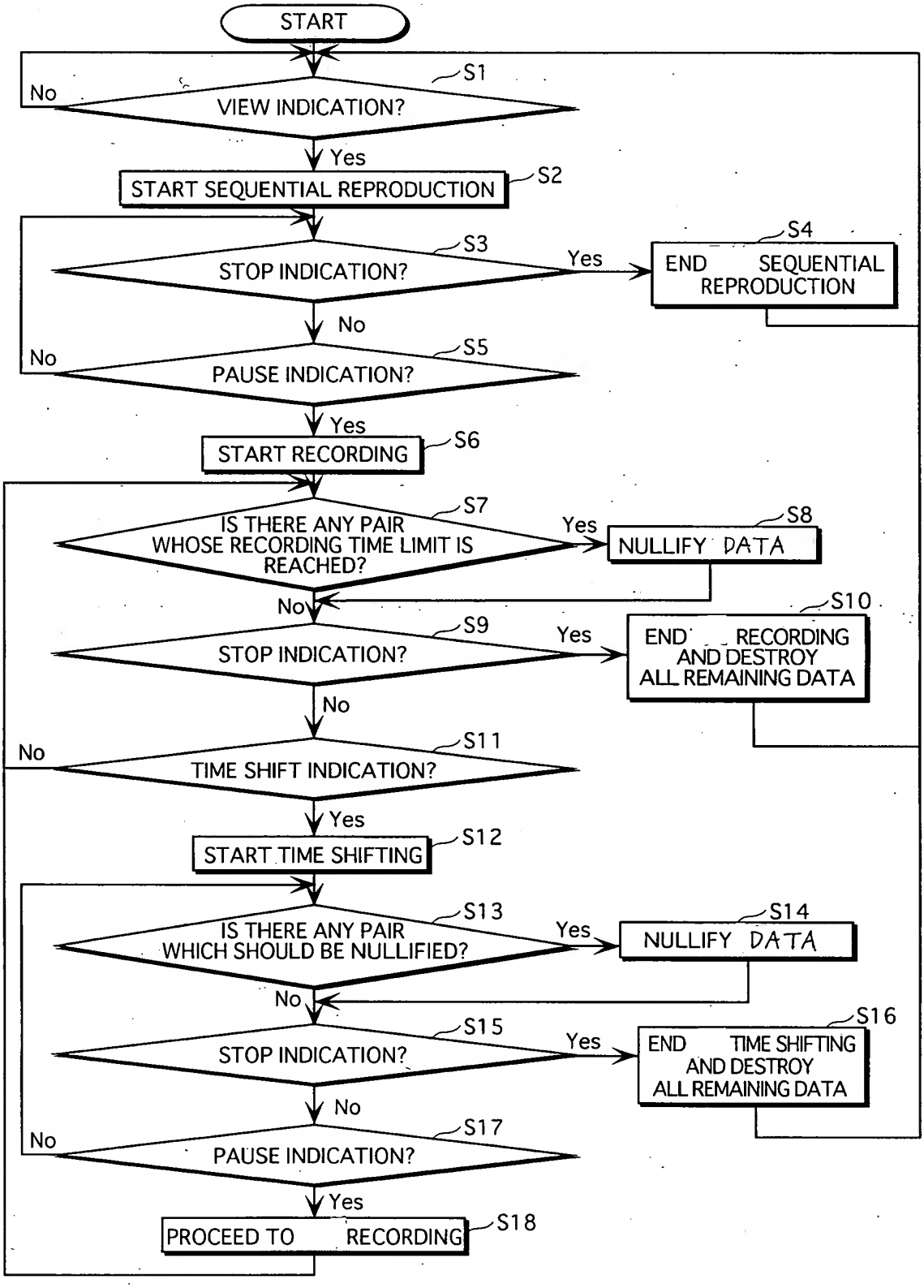

START
S1
VIEW INDICATION?
No
Yes
START SEQUENTIAL REPRODUCTION
S2
S3
STOP INDICATION?
Yes
S4
END SEQUENTIAL REPRODUCTION
No
S5
PAUSE INDICATION?
No
Yes
START RECORDING
S6
S7
IS THERE ANY PAIR WHOSE RECORDING TIME LIMIT IS REACHED?
Yes
S8
NULLIFY DATA
No
S9
STOP INDICATION?
Yes
S10
END RECORDING AND DESTROY ALL REMAINING DATA
No
S11
TIME SHIFT INDICATION?
No
Yes
START TIME SHIFTING
S12
S13
IS THERE ANY PAIR WHICH SHOULD BE NULLIFIED?
Yes
S14
NULLIFY DATA
No
S15
STOP INDICATION?
Yes
S16
END TIME SHIFTING AND DESTROY ALL REMAINING DATA
No
S17
PAUSE INDICATION?
No
Yes
PROCEED TO RECORDING
S18

FIG.4

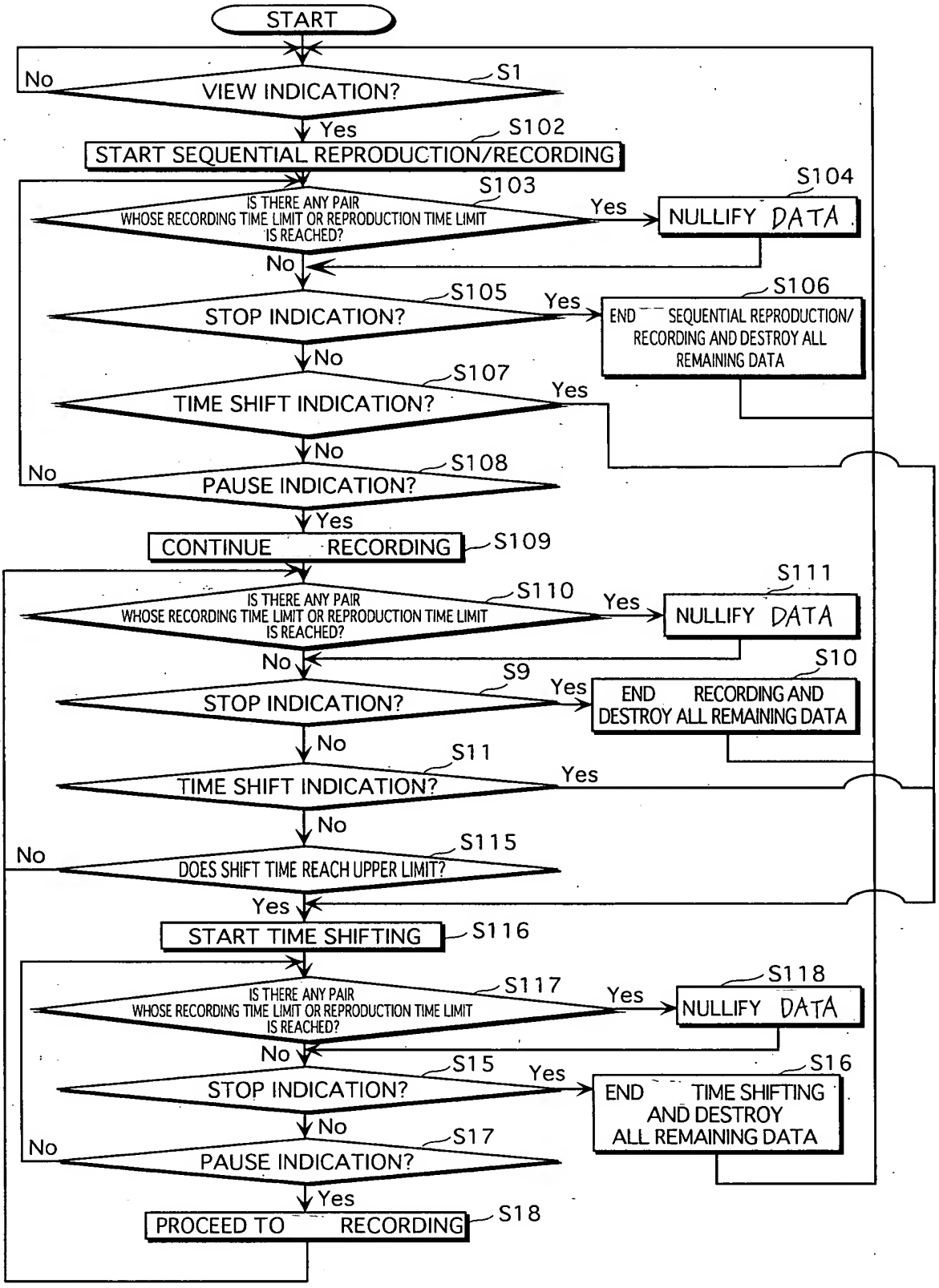

START
S1
VIEW INDICATION?
No
Yes
S102
START SEQUENTIAL REPRODUCTION/RECORDING
S103
IS THERE ANY PAIR WHOSE RECORDING TIME LIMIT OR REPRODUCTION TIME LIMIT IS REACHED?
Yes
S104
NULLIFY DATA
No
S105
STOP INDICATION?
Yes
S106
END SEQUENTIAL REPRODUCTION/ RECORDING AND DESTROY ALL REMAINING DATA
No
S107
TIME SHIFT INDICATION?
Yes
No
S108
PAUSE INDICATION?
No
Yes
CONTINUE RECORDING
S109
S110
IS THERE ANY PAIR WHOSE RECORDING TIME LIMIT OR REPRODUCTION TIME LIMIT IS REACHED?
Yes
S111
NULLIFY DATA
No
S9
STOP INDICATION?
Yes
S10
END RECORDING AND DESTROY ALL REMAINING DATA
No
S11
TIME SHIFT INDICATION?
Yes
No
S115
DOES SHIFT TIME REACH UPPER LIMIT?
No
Yes
START TIME SHIFTING
S116
S117
IS THERE ANY PAIR WHOSE RECORDING TIME LIMIT OR REPRODUCTION TIME LIMIT IS REACHED?
Yes
S118
NULLIFY DATA
No
S15
STOP INDICATION?
Yes
S16
END TIME SHIFTING AND DESTROY ALL REMAINING DATA
No
S17
PAUSE INDICATION?
No
Yes
PROCEED TO RECORDING
S18

FIG. 5

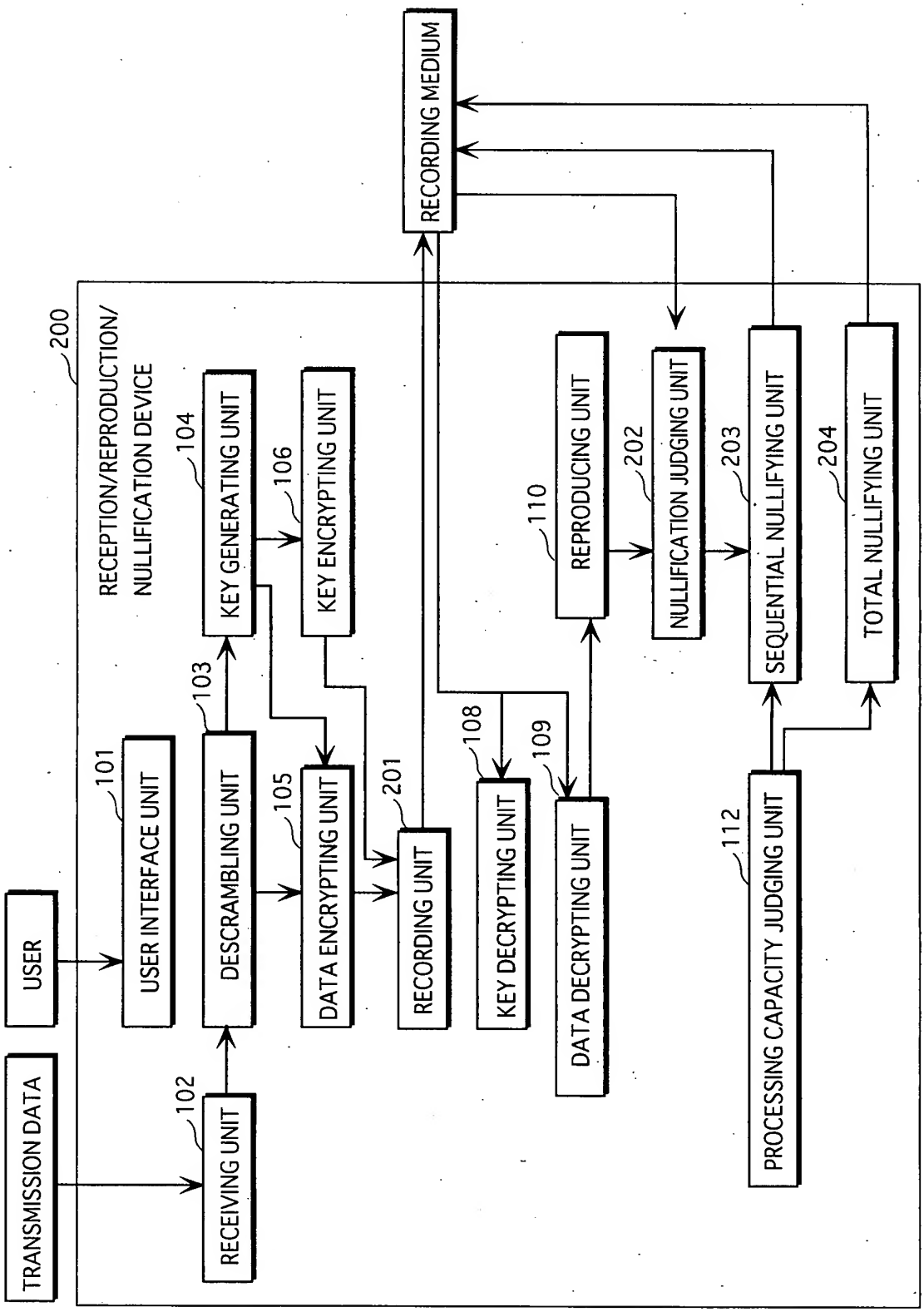

RECORDING MEDIUM
200
RECEPTION/REPRODUCTION/
NULLIFICATION DEVICE
USER
TRANSMISSION DATA
101
USER INTERFACE UNIT
102
RECEIVING UNIT
103
DESCRAMBLING UNIT
104
KEY GENERATING UNIT
105
DATA ENCRYPTING UNIT
106
KEY ENCRYPTING UNIT
201
RECORDING UNIT
108
KEY DECRYPTING UNIT
109
DATA DECRYPTING UNIT
110
REPRODUCING UNIT
202
NULLIFICATION JUDGING UNIT
203
SEQUENTIAL NULLIFYING UNIT
204
TOTAL NULLIFYING UNIT
112
PROCESSING CAPACITY JUDGING UNIT

FIG.6

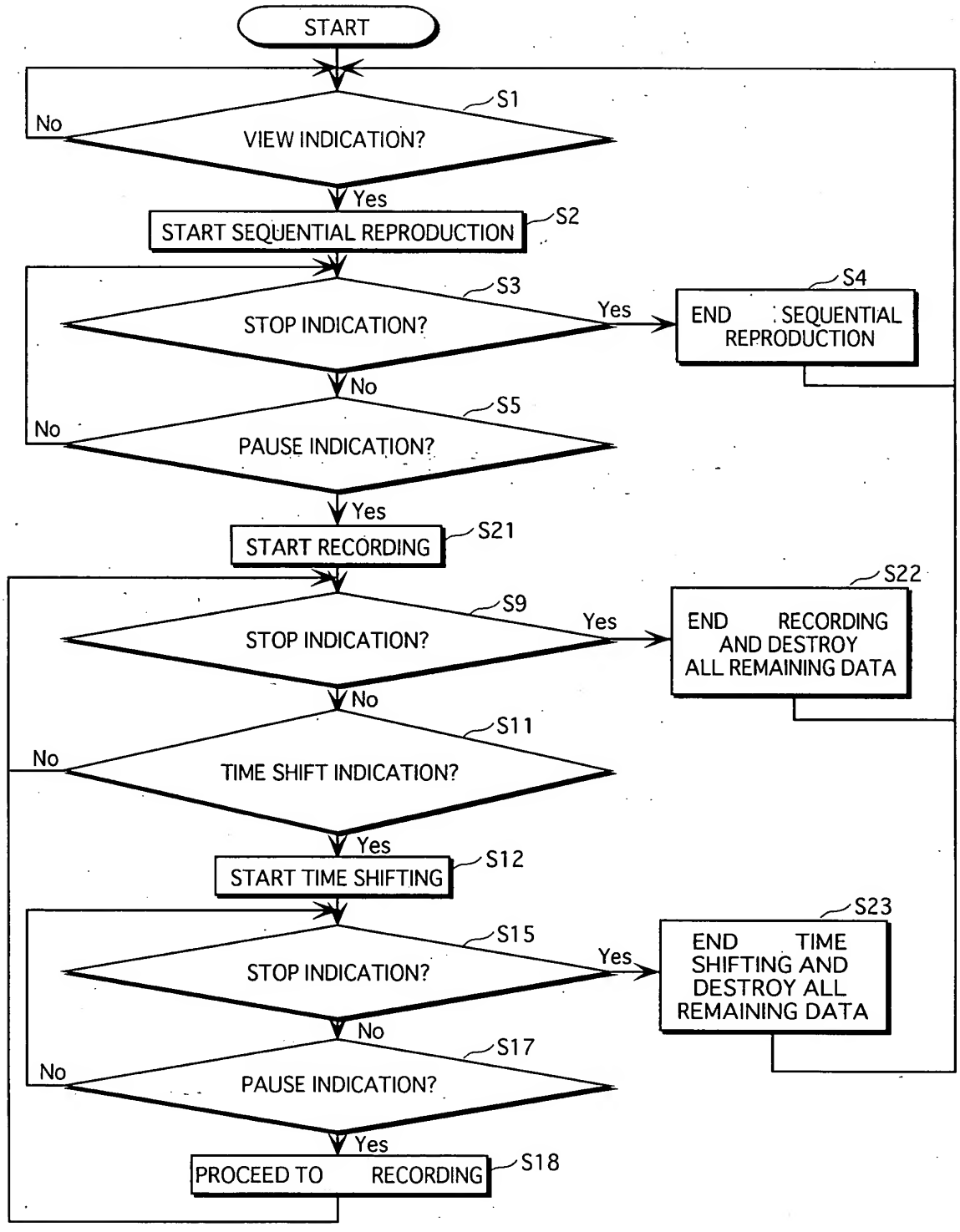

START
S1
VIEW INDICATION?
No
Yes
START SEQUENTIAL REPRODUCTION
S2
S3
STOP INDICATION?
Yes
S4
END SEQUENTIAL REPRODUCTION
No
S5
PAUSE INDICATION?
No
Yes
START RECORDING
S21
S22
S9
STOP INDICATION?
Yes
END RECORDING AND DESTROY ALL REMAINING DATA
No
S11
TIME SHIFT INDICATION?
No
Yes
START TIME SHIFTING
S12
S23
S15
STOP INDICATION?
Yes
END TIME SHIFTING AND DESTROY ALL REMAINING DATA
No
S17
PAUSE INDICATION?
No
Yes
PROCEED TO RECORDING
S18

FIG. 7

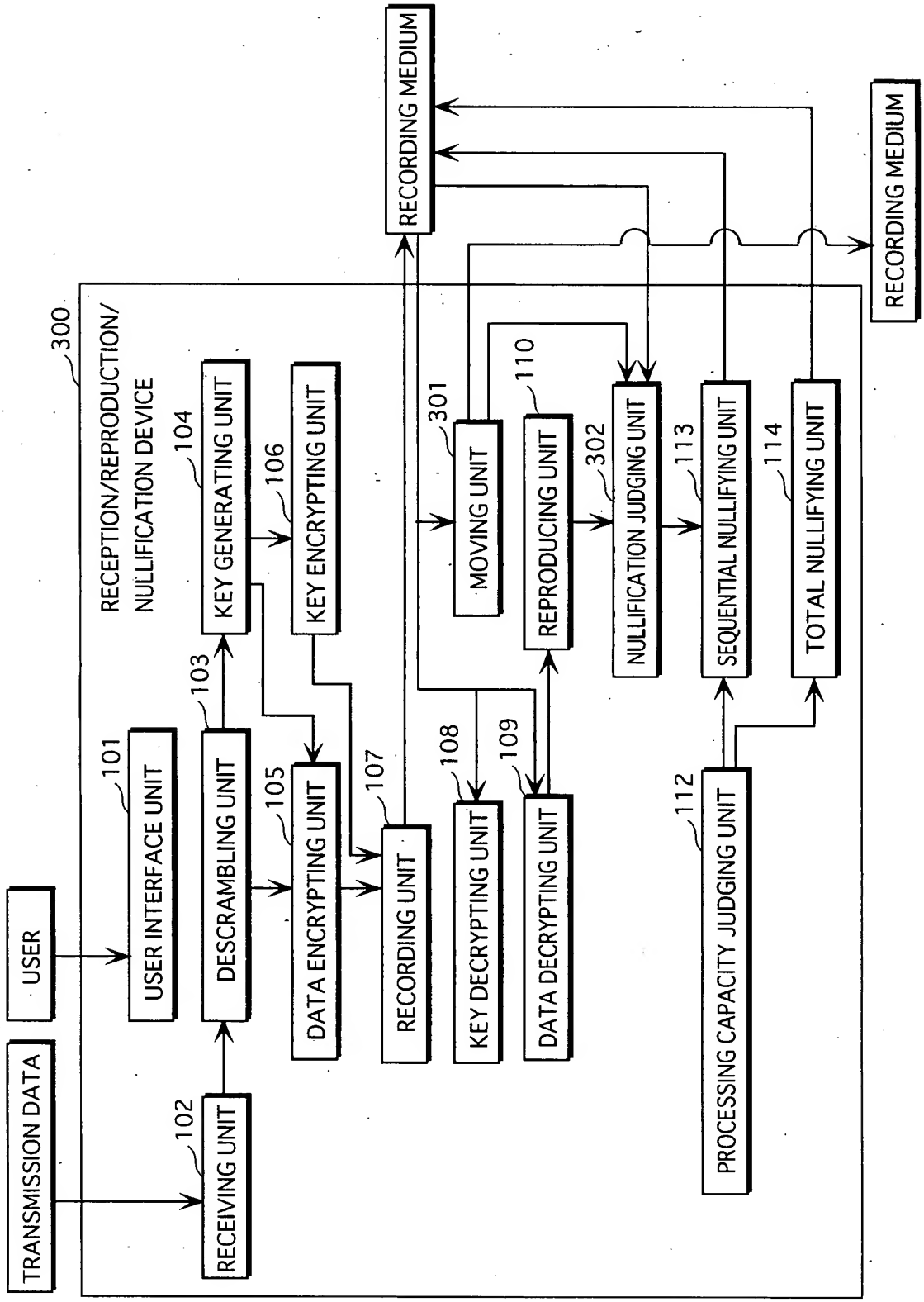
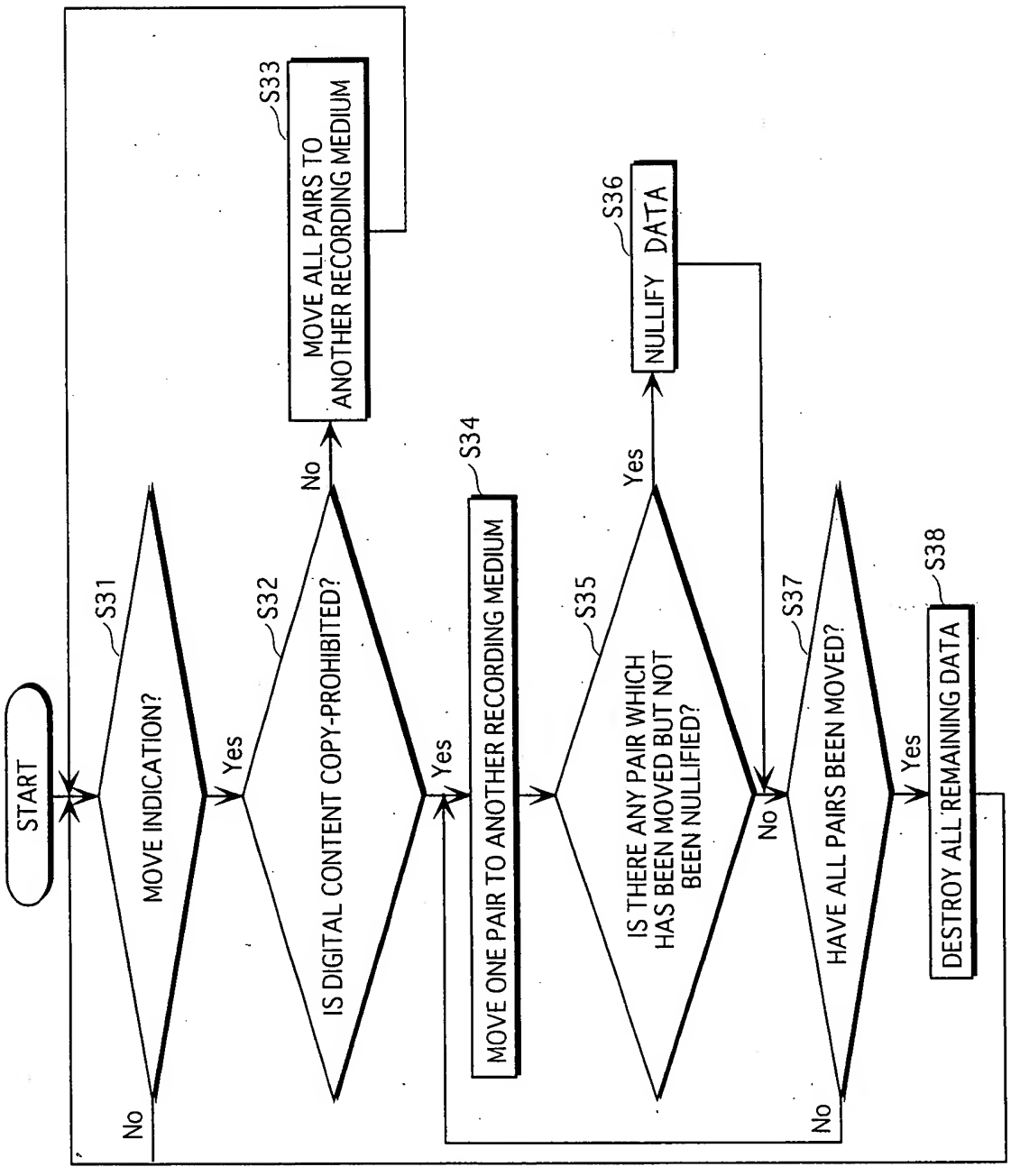

TRANSMISSION DATA
USER
RECEIVING UNIT
USER INTERFACE UNIT
DESCRAMBLING UNIT
KEY GENERATING UNIT
KEY ENCRYPTING UNIT
DATA ENCRYPTING UNIT
RECORDING UNIT
KEY DECRYPTING UNIT
DATA DECRYPTING UNIT
MOVING UNIT
REPRODUCING UNIT
NULLIFICATION JUDGING UNIT
SEQUENTIAL NULLIFYING UNIT
TOTAL NULLIFYING UNIT
PROCESSING CAPACITY JUDGING UNIT
RECORDING MEDIUM
RECORDING MEDIUM
RECEPTION/REPRODUCTION/
NULLIFICATION DEVICE
300
101
102
103
104
105
106
107
108
109
110
112
113
114
301
302

FIG. 8


START
S31
MOVE INDICATION?
No
Yes
S32
IS DIGITAL CONTENT COPY-PROHIBITED?
No
S33
MOVE ALL PAIRS TO ANOTHER RECORDING MEDIUM
Yes
S34
MOVE ONE PAIR TO ANOTHER RECORDING MEDIUM
S35
IS THERE ANY PAIR WHICH HAS BEEN MOVED BUT NOT BEEN NULLIFIED?
Yes
S36
NULLIFY DATA
No
S37
HAVE ALL PAIRS BEEN MOVED?
No
Yes
S38
DESTROY ALL REMAINING DATA